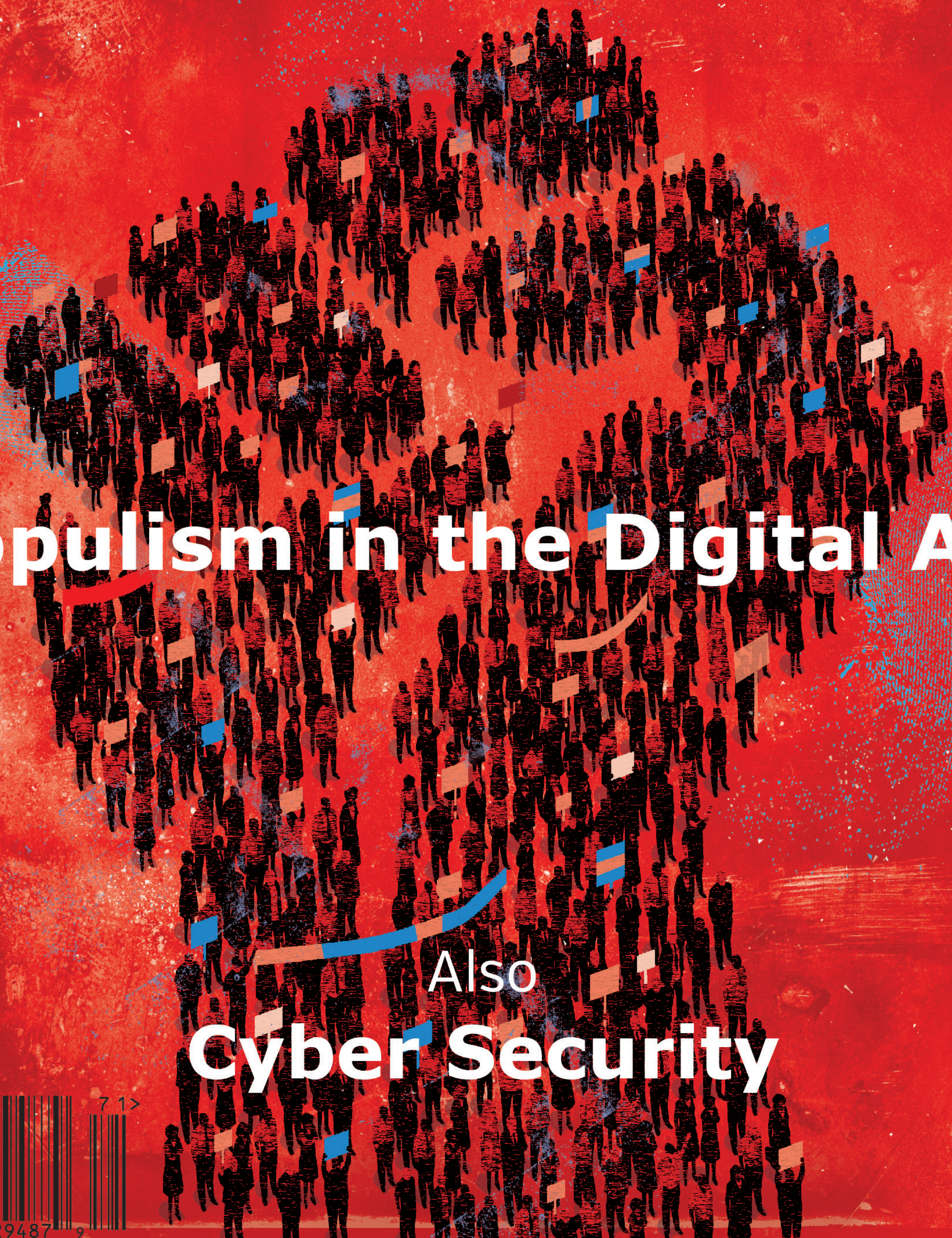
Spring 2017

Volume 2, Issue 1

IAF

International Affairs Forum



Populism in the Digital Age

Also

Cyber Security

contents

spring 2017

POPULISM IN THE DIGITAL AGE

CYBER SECURITY

International Affairs Forum

Printed in the U.S.A.
A publication of the Center for International Relations
1629 K St. NW #300, Washington DC 20006
202-821-1832 email: editor@ia-forum.org

Submit your Editorial or Essay to
editor@ia-forum.org

www.ia-forum.org

International Affairs Forum

Special Themed Issue: Editors' Introduction

This issue of International Affairs Forum focuses on the themes of Populism in the Digital Age and Cyber Security. Both topics have been at the forefront of recent news and, looking ahead, should continue to warrant high interest. This issue presents a wide a range of article/ opinion pieces and interviews from practitioners and academics from around the world. We are also very pleased to include two contributions from winners of the International Affairs Forum Student Writing Competition (found in the cyber security section).

Populist parties and sentiments have become increasingly prominent in U.S. and European elections. Moreover, the expanding use of digital communications, including social media platforms such as Twitter, have provided populist movements with other channels to spread their messages. To explore this, the first section of this issue explores not only populism around the world, but also the impact of digital communications on their efforts.

Coverage of populism in the digital age transverses the general discussion of populist movements (Prof. Cas Mudde discussing the definition of populism and current trends), to regional topics including Prof. Cristóbal Rovira Kaltwasser's analysis of populism in Latin America, analysis of populism in Europe (Stefan Lehne, Prof. Fabian Vichow (Germany), Dr. Tsveta Petrova (Eastern Europe), Prof. Giovanna Campani (Italy)); discussion of Australia's One Nation Party (Prof. Zareh Ghazarian); to an examination of anti-Chinese populism in Africa (Prof. Steve Hess). Other pieces discuss populism in the U.S., from Dr. Harry C. Boyte on facets of U.S. populism and movements starting in the 1960s to the present, to Prof. John Abromeit discussing U.S. and European populist movements; to Prof. Kristin Haltinner's analysis of the Tea Party and its effect on the Trump election campaign. Focusing more specifically on our topic, Dr. Sven Engesser discusses the role of media in populist movements

Cyber security is being tested with increasing regularity and intensity. The recent worldwide-level WannaCry ransomware attack and cyber strategies to influence elections touch on the many potential effects of cyber attacks. Contributions to this section include discussions of cyber policies and threats (Dr. John W. Singer), deterring cyber attacks (Sico van der Meer), cyber risk (Nadia Kostyuk), cyber conflict (Miguel Alberto Gomez), and the "hacking back" debate (Tim Ridout). Dr. Alexander Crowther presents an analysis of NATO cyber security efforts while data integrity is examined by Edward M. Stroz, and an analysis of safeguarding financial data is presented by Tim Maurer and Steven Nyikos. In examining the technical aspects of cyber security, Prof. Jason Hong discusses cyber security related behaviors and Anup Ghosh discusses machine learning and its effects to increase cyber security efforts. Finally, winners of the International Affairs Forum Student writing competition analyze the EU's cyber policies (Sophie Barnett) and the issue of child porn on the Darknet (Cohen).

The core values for the publication are:

- We aim to publish a range of op-ed pieces, interviews, and short essays, alongside longer research and discussion articles that make a significant contribution to debates and offer wider insights on topics within the field;
- We aim to publish content spanning the mainstream political spectrum and from around

the world;

- We aim to provide a platform where high quality student essays are published (winners of the IA Forum Student Writing Competition);
- We aim to publish the journal bi-annually;
- We aim to provide submitting authors with feedback to help develop and strengthen their manuscripts for future consideration.

All of the solicited pieces have been subject to a process of editorial oversight, proof-reading, and publisher's preparation, as with other similar publications of its kind.

We also welcome unsolicited submissions for consideration alongside the solicited pieces. In addition, the publication holds a student writing competition, seeking the best student pieces for publication in the journal along with our distinguished contributors.

We hope you enjoy this issue and encourage feedback about it, as it relates to a specific piece or as a whole. Please send your comments to: editor@ia-forum.org

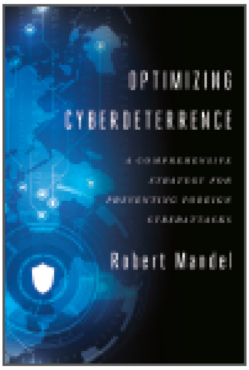
DISCLAIMER

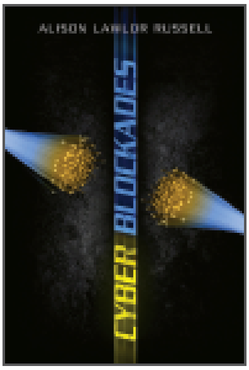
International Affairs Forum is a non-partisan publication that spans mainstream political views. Contributors express views independently and individually. The thoughts and opinions expressed by one do not necessarily reflect the views of all, or any, of the other contributors.

The thoughts and opinions expressed are those of the contributor alone and do not necessarily reflect the views of their employers, the Center for International Relations, its funders, or staff.

POPULISM IN THE DIGITAL AGE

NEW FROM GEORGETOWN


OPTIMIZING
CYBERDETERRENCE
A COMPREHENSIVE STRATEGY FOR PREVENTING FOREIGN CYBERATTACKS
Robert Mandel

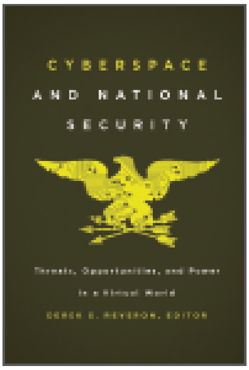


Optimizing Cyberdeterrence

A Comprehensive Strategy for
Preventing Foreign Cyberattacks
Robert Mandel
978-1-62616-413-0, paperback, $32.95
978-1-62616-412-3, hardcover, $64.95
978-1-62616-414-7, ebook, $32.95

Cyber Blockades

Alison Lawlor Russell
978-1-62616-112-2, paperback, $29.95
978-1-62616-111-5, hardcover, $49.95
978-1-62616-113-9, ebook, $29.95



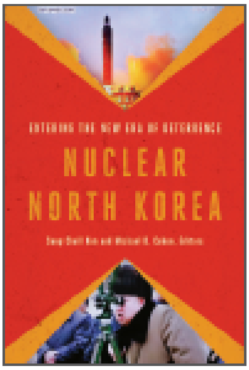
Georgetown Journal of International Affairs
International Engagement on Cyber VI
Assessing Cyber Strategies

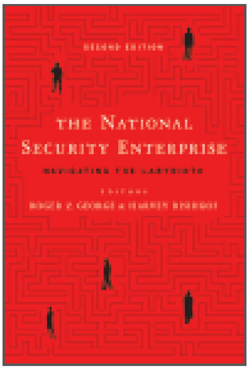
Cyberspace and National Security

Threats, Opportunities, and Power in a Virtual World
Derek S. Reveron, Editor
978-1-58901-918-6, paperback, $29.95
978-1-58901-919-5, ebook, $29.95

Georgetown Journal of International Affairs

International Engagement on Cyber VI
Volume 17, No. 3
Ian Prasad Philbrick and Andrew McCoy, Editors
978-1-62616-388-1, paperback, $17.95


ENTERING THE NEW ERA OF DETERRENCE
NUCLEAR
NORTH KOREA
Sung Chull Kim and Michael D. Cohen, Editors



North Korea and Nuclear Weapons

Entering the New Era of Deterrence
Sung Chull Kim and Michael D. Cohen, Editors
978-1-62616-453-6, paperback, $32.95
978-1-62616-452-9, hardcover, $64.95
978-1-62616-454-3, ebook, $32.95

The National Security Enterprise

Navigating the Labyrinth
Second Edition
Roger Z. George and Harvey Rishikof, Editors
978-1-62616-440-6, paperback, $36.95
978-1-62616-439-0, hardcover, $72.95
978-1-62616-441-3, ebook, $36.95

GEORGETOWN UNIVERSITY PRESS
800.537.5487 • www.press.georgetown.edu

AVAILABLE AS EBOOKS FROM SELECT EBOOK RETAILERS.

FOLLOW US @GUPRESS

Populism...a threat to liberal democracy?

Interview with Professor Cas Mudde
University of Georgia

What does populism present to liberal democracy?

I define populism as a thin-centered ideology that considers society to be ultimately separated into two homogeneous and antagonistic groups, "the pure people" and "the corrupt elite." Populism argues that politics should be an expression of the volonté generale (general will) of the people.

As such, populism is pro-democracy, i.e. popular sovereignty and majority rule, but anti-liberal democracy, (democracy plus minority rights, pluralism, and rule of law). Because the essence of populism is monism, in which divisions within "the people" are considered secondary or non-existent, as well as moralism, the distinction between "pure" and "corrupt" populism will often lead to polarization and marginalization, if not outright repression, of political minorities, who are not seen as "opponents" but as enemies.

Can populism have any positive effects populism on a liberal democracy?

Populism can certainly have positive effects, particularly in opposition. Populists often ask the right questions, but provide the wrong answers. They challenge established parties on previously unaddressed issues, that part of the population believes has not been sufficiently addressed, such as European integration and immigration in Western Europe in the 1990s.

In addition to the (re-)politicization of "forgotten" issues, populists can help re-integrate "forgotten" groups of voters, i.e. people who have been largely ignored by the mainstream parties such as the rural population or the white working class.

What are your thoughts on the current state of populism in Europe?

Populism is stronger than it has ever been in Europe, but almost no successful populist party lives off of populism alone. The most successful subgroup of populist parties are the so-called populist radical right, who combine populism with authoritarianism and nativism – parties such as the Austrian Freedom Party (FPÖ), the French National Front (FN), and the Dutch Party for Freedom (PVV). Their success is at least as much the result of their nativism and authoritarianism as of their populism. Similarly, the few successful left-wing populist parties in Southern Europe, notably Podemos in Spain and SYRIZA in Greece, profit both from their populism and from their "socialist" socio-economic agenda.

How have European populist movements and party leaders (e.g., Geert Wilders) leveraged digital means such as social media, apps, and websites as well as traditional mass media outlets to further their agenda? What about populist leaders currently in power (e.g., Viktor Orban)?

Some populist leaders are very adept at using social media. For example, Beppe Grillo, the founder of Italy's Five Star Movement (M5S), ran the most popular blog in Italy before starting his party. Party for Freedom (PVV) leader Geert Wilders dominated Dutch politics on Twitter well before Donald Trump even considered running for president. But other parties, like the French

National Front (FN), don't have a remarkable social media presence. Most political parties, populist or not, still depend on traditional media. Social media can help them to bypass the gatekeepers of traditional media, and set their own political agenda by dominating the social media – after all, the traditional media will not ignore social media "sensations" (see the so-called "alt-right" in the United States). Wilders was so successful in this strategy that he didn't give interviews to traditional media, as they would just run with his tweets and force the established politicians to respond to them.

The Hungarian Prime Minister Viktor Orbán is different. He doesn't have a particularly strong social media presence nor does he need one. He came to power on the basis of a very broad "civic movement", which almost created a parallel society in opposition. After coming to power, he streamlined the traditional media through a broad range of economic and political measures (paralleling those of Vladimir Putin's in Russia). Today, most national media outlets are uncritically pro-Orban, while the media in opposition are marginalized.

President Trump is considered by many to have won the election by running a populist campaign. Do you agree? In what ways do you think he resembles a populist and in what ways, not?

Donald Trump started out as an anti-establishment politician, but not as a populist. In the first months he world barely mention "the people" and mainly sold "The Donald." It really was all about him: he made "the greatest deals" and "only he" could "make America great again." That was more so an elitist form of anti-establishment politics. His campaign adopted a more populist tone after he secured the Republican nomination, undoubtedly under the influence of his campaign manager, Steve Bannon. In the last months of his campaign, Trump increasingly presented himself as the voice of the people that would give politics back to the people, and he has continued to do so as president. His inauguration speech was profoundly populist.

Populism is stronger than it has ever been in Europe, but almost no successful populist party lives off of populism alone.

How effective do you believe digital campaigns using media such as Twitter actually had on influencing citizens to vote for Mr. Trump?

I am not sure how important the digital campaigns were. You cannot see these campaigns independent of decades of more traditional conservative media, most notably Fox News and talk radio (e.g., Glenn Beck, Rush Limbaugh, Michael Savage). They influenced Trump voters much more, and made them susceptible to even more conservative, and radical right, digital media like Breitbart News and Infowars. Moreover, the pro-Trump camp was very closely linked to the anti-Clinton campaign, which has its origins in the 1990s, well before the emergence of digital media.

Do you believe there are any misperceptions about voters who supported Trump and Brexit?

Are most of them truly supporters of populism? I believe that the majority of Trump voters first and foremost voted for the only remaining viable candidate of their party. They would also have voted for Ted Cruz or Marco Rubio. That is not to say that they don't support many of Trump's nativist, authoritarian, and populist sentiments – survey after survey shows they do – but they consider Trump too extreme and would have preferred someone else.

I think Brexit is not much different: the majority were Tory voters, not UKIP voters. Hence, you cannot equate the Brexit and Trump electorate with those of the FN or PVV. At the very least, the populist radical right campaign didn't discourage Brexit and Trump voters from supporting them, showing that while the majority of the population may not hold populist values, they tolerate them.

You've expressed the need for greater research about youth in their progression to embrace populist movements. How much is currently known? Do you think gathering and analyzing digital data – including social media – could/should be used to support such studies?

We need more research on many issues related to extremism and democracy – right, left and center – but also much better integration and dissemination of this research. This is why I am currently fundraising to create a, provisionally named, Center for Analysis of Democracy and Extremism (CADE) at the University of Georgia, which will stimulate new research, integrate new and old scholars, and connect them to journalists and practitioners. Research about youth is crucial here, as most people develop their (populist radical right) attitudes, and join the more extreme groups in their late teens and early twenties. Digital data is part of that research. We know that social media are more important for younger cohorts, and subcultures attract people through attractive propaganda and the use of strong symbols. But it would also include more traditional surveys, preferably of the same groups over many years (e.g., 13 to 18-year olds), as well as participant observation of subcultures (like skinheads, followers of white power music) and youth branches of populist radical right parties.

How large a factor has migration been to current populist movements in Europe and the U.S.?

Immigration has always been a major issue for populist radical right parties – though not for left-wing populist parties like Podemos or SYRIZA, which tend to be among the most pro-immigrant parties in Europe. But the link between the level of immigration and the electoral success of populist radical right is complex. Opposition to immigration has both socio-economic and socio-cultural grounds, which are interrelated. Economic anxiety is socio-culturally translated. For example, many people worry about the state of the economy or the welfare state, because they see immigrants as "undeserving" of (good) jobs and welfare provisions. On the other hand, there are purely socio-culturally issues, such as the role of Islam in western societies, which have more to do with integration than immigration, as many Muslims are naturally-born citizens of West European countries.

Cas Mudde is Associate Professor, School of Public and International Affairs (SPIA), University of Georgia, USA; Researcher, Center for Research on Extremism (C-REX), University of Oslo, Norway; and Co-editor European Journal of Political Research.

His recent books are: *On Extremism and Democracy in Europe* (Routledge, 2016), *The Populist Radical Right: A Reader* (Routledge, 2017), *SYRIZA: The Failure of the Populist Promise* (Palgrave Macmillan, 2017), *Populism: A Very Short Introduction* (Oxford UP, 2017), *The Far Right in America* (Routledge, 2017)

Contextualizing Populism in Latin America: populist movements within the changing political and technological landscapes

Interview with Professor Cristóbal Rovira Kaltwasser
Diego Portales University

Through your research, what commonalities have you identified between populist groups in Latin America, Europe and North America?

Populism is a very contested concept, and the approach that I have been following with Professor Cas Mudde, and also with many other colleagues, is to define populism as a specific set of ideas that considers society to be separated between "the pure people" and "the corrupt elite", and which argues that popular sovereignty should be defended by all means. In this sense, our argument is that all populist actors adhere to this very specific set of ideas. It doesn't matter if they're right wing or left wing. You can analyze different populist actors in North America, South America, in Europe, based on that definition.

If we think about the commonalities, there are at least three that are worth mentioning. The first one is that all populist actors try to politicize, or in some cases repoliticize, certain issues that the political establishment has not been taking into account. For example, in the case of Europe, it's very clear that immigration has been a very important issue for a big part of the population, but mainstream political parties have not been dealing with this issue. Not by chance, what populists writing in Breitbart News have tried to do is to politicize that issue. In the case of Latin America, it's much more related to inequality, poverty, and some of the consequences of neoliberal economic policies. What all these cases have in common is that they try to (re) politicize certain issues that are relevant to some constituencies.

The second similarity is polarization, which is related to the capacity of populist forces to (re) politizice certain issues that are relevant for the electorate. It is important to take into account that populist actors try to to polarize not only the electorate, but also the political debate. This is because they try to put into the public agenda certain topics that, to a certain extent, are uncomfortable for the political establishment. In the case of Europe, this is very clear, because since the '90s we have seen a growing convergence between mainstream left and

> *[we] define populism as a specific set of ideas that considers society to be separated between "the pure people" and "the corrupt elite", and which argues that popular sovereignty should be defended by all means.*

mainstream right political parties. What populist parties do in Europe, on the left side and the right side, is to generate polarization.

The third and last commonality is the difficulties between populism and liberal democracy. I would argue that it doesn't matter if we are looking at leftist or rightist populist actors: all of them have a very ambivalent relationship with the political regime, and they can generate both positive and negative effects on liberal democracy.

How would you characterize recent trends in Latin American populist movements?

Since around the end of the 1990s, we have seen the rise of a new wave of populism, which is a leftist wave of radical populist leaders. The key examples are Hugo Chávez in Venezuela, Evo Morales in Bolivia, and Rafael Correa in Ecuador. During the 2000s, all these leaders were relatively successful in terms of winning elections. But what we are seeing nowadays is that most of these populist projects are facing a very difficult time.

There are two reasons why these populist projects are facing growing challenges in the electoral arena today. One is the end of the commodity boom. During the 2000s, Latin America had very good rates of economic growth, related to the export of commodities which had very good prices in the international market. So, for ten years, these populist leaders had the advantage of having a lot of money to be distributed for poor people. This is not the case anymore. The second issue is corruption. We have seen the coming into light of several corruption scandals [uncovered] in Ecuador, in Venezuela and, to a certain extent, also in Bolivia. This, of course, damages the legitimacy of these populist leaders and their political projects.

It's still an open question how things are going to evolve over time in these countries, but the overall impression that I have, and also shared by many analysts, is that these populist leaders are facing growing challenges at the domestic and external levels.

The election of President Trump has had ripple effects in the Americas, particularly regarding potential migration policy. How do you think his election has affected populist movements, if at all, in Latin America?

To a certain extent, I think Trump is a blessing for populist actors in Latin America because he is a very radical populist right-wing actor, who is generating polarization inside and outside of the U.S. Given that many of these leftist populist leaders in Latin America have a very difficult relationship with the U.S., having Trump in power is a blessing for them. Now they can say, "we have always told you that the U.S. is a very bad country which is against us." The rhetoric of Trump will help them to boost that type of argument. Obama was much trickier for leftist populists, because he had a much more pluralist take and a tendency to defend multi-polar arguments. Trump is the opposite. So, from a populist perspective in Latin America, the coming to power of Trump is good for the moral and Manichean distinction between "the people" and "the elite."

What have you seen in populist groups in Latin America in terms of utilization of media to support their platforms? In particular, have you seen much activity in this regard concerning embracing digital media?

I would say, yes and no. It depends a bit on the cases. Venezuela, for example, is a very clear instance in which Chávez was in the media the whole time. He used Twitter but he was also using television. In the case of Evo Morales in Bolivia, digital media plays a role, but not that big. So, in this sense, I'm a bit skeptical about saying that we can see across all the cases in Latin America that digital media plays a major role.

But a commonality we can see is that as soon as these leaders come to power, they try to control the media system. For example, they start to close media outlets, they try to put barriers against newspapers and TV channels that develop critical arguments, and they also develop new media outlets to promote their own ideas. This is what some authors have called a sort of "populist media complex", which tries to reinforce the arguments that these leaders advance. Of course, this is related to the question of the difficult relationship with populism and liberal democracy.

However, this is not only a Latin American phenomenon, but rather a relatively common phenomenon around the world. If you look across different cases, when you have populist leaders in power, they can use various mechanisms to restructure the political regime. Nevertheless, this occurs only when they are very powerful, meaning that they get more than fifty percent of the vote and thus control the executive and/or legislative branch. For example, with Viktor Orbán in Hungary, there is a similar situation, in which he has reformed the Constitution to give him power to control media outlets.

In recent political elections, the Brexit vote, the Trump win, and the vote in the Netherlands, many pollsters and pundits have been wrong in their predictions. It would appear that measuring populism has been challenging. Is that a fair statement?

Measuring populism has been a tricky business, in part because of the absence of a common definition. Nevertheless, my impression is that there is growing consensus around an ideational approach to populism; i.e., the concept that I have developed with Professor Mudde and also the proposals of various colleagues who advance similar definitions. This sort of consensus within academia is helping to create new ways of measuring populism in terms of looking at both the supply side and the demand side. For example, by employing surveys one can examine to what extent the populist set of ideas is widespread across the population.

The tricky part with these measures, based on the research that various colleagues have been doing, is that the populist set of ideas seems to be very widespread across most countries of the world. In fact, we have measures for Chile, the Netherlands the U.S., and other countries. And the empirical evidence shows that many of us have this populist set of ideas in our mindsets. The key question is, when do these ideas have an impact on our voting behavior? My impression is that this set of ideas is normally latent. So it's dormant and it's only under very specific circumstances that a vast section of the population would rely on the populist set of ideas to take political decisions. In other words, it's only under very specific circumstances that these attitudes or these ideas get activated. This is what we are trying to figure out now through new research.

For example, imagine that we are Greek voters, and we are facing the economic crisis, witness huge corruption scandals, and realize that the European Union and the International Monetary Fund are imposing austerity measures. I think most of us would say, this is enough, let's get rid of "the elite" and "the people" should rule. But this is a very specific context.

An argument that I have been developing with other colleagues is that a populist can really get into power – by this meaning more than 50% of the vote – only under very specific circumstances. There has to be a major crisis, not necessarily in terms of an economic crisis, but a crisis of democratic representation where so many people are upset with what is going on that they will rely on the populist set of ideas, and start voting en masse for a populist actor.

Going back to your question about measuring populism and the problem with pollsters, we can examine this when asking whether someone will vote for a populist candidate. For example, in the case in the U.S., many people ended up voting for Trump, but they didn't say that. That's one of the tricky parts with populism, and it goes back to this debate that we had before with the activation of populist attitudes. Returning to the example of Greece, first, we know that most people are a bit reluctant to vote for populist because they know that this is a very radical ideology. Because of that, this is a delicate part with measurement. It might be that many people end up voting for populist actors, but they're not very keen on saying that openly. That's one of the problems with the measurement that we have been seeing across different countries. This is the tricky part with measuring the populist set of ideas and is related to a sort of negative social desirability bias.

The other point that I want to develop is, for example, if you look at the case of the Dutch election, the media was arguing that, in terms of the number of votes, the winner is going to be Wilders. We have seen that he received around 15% of the vote. It's not huge, but it's still a big thing. But what is really interesting in that case is that the turnout level went up. I think this is probably one of the positive effects of populism. When you have growing polarization because of populism, many people start to think, this is a problematic issue. So if many people are going to vote, for example, for Wilders, and you're against his political project, you will say, it's important that I go to the polls, and I raise my opinion. So in this sense, the impact of populism on democracy is not always and not necessarily negative, because it generates more engagement by both sides, those who are in favor of populism, but at the same time, those who are against populism. In a sense, it makes democratic debate a bit more lively.

Cristóbal Rovira Kaltwasser is an associate professor at the School of Political Science of the Diego Portales University (Chile). He received his PhD in political science from the Humboldt-University of Berlin in 2008. Professor Rovira Kaltwasser's main area of research is comparative politics and he has a special interest in the ambivalent relationship between populism and democracy. He has also worked as a research fellow at the University of Sussex, the Social Science Research Center Berlin (WZB) and the Human Development group of the Chilean Bureau of the United Nations Development Programme (UNDP).

Populism: the risks and impact on European states

Interview with Stefan Lehne
Carnegie Europe

You've stated that there are six big risks from populism. Would you expand?

The American political scientist Francis Fukuyama has said that "populism is the label political elites attach to policies supported by ordinary citizens that they don't like." And it is true that populism should not be regarded as a pathology, but rather as an inherent element of democracy. When important concerns of the people are not addressed by the elites, the populist movements tend to form to challenge the establishment. Their ideas can rejuvenate democracy, bring new people into the political process, and adjust the political system to societal change.

But there are features common to many populist movements which are far less benign.

A. They are often based on a crude division between "us" (the pure people) and "them" (the corrupt elites and/or the foreigners). They often claim absolute moral superiority and possession of the whole truth. That makes them reject the legitimacy of the opponent. For the same reason, they are often inherently opposed to compromise and are unwilling to participate constructively in the political process.

B. Their way of operating often results in a decline in rational debate about political issues. There have always been a lot of lies in politics, but what we have witnessed, for instance, in the Trump or in the Brexit campaigns has a new quality. Observers have spoken of the post-truth age.

C. Populist movements are often led by charismatic leaders and have little internal democracy and accountability. These leaders tend to develop personality cults and, when they come to power, they often turn authoritarian. There is also a high risk of corruption and abuse of power.

D. Populist movements often turn against representative democracy and advocate instead a shift towards direct democracy on all levels. This offers them useful occasions for mobilization and frequently catches the elites on the back foot. But without an in-depth preparation through rational debate, as for instance is the long-standing practice in Switzerland, referenda often are influenced by factors extraneous to the issue at stake and end with arbitrary outcomes. You always get an answer, but often not to the question that has been asked.

E. For many populist movements, national sovereignty is the highest good. They are thus intrinsically mistrustful of international rules and tend to adopt aggressive "zero-sum" foreign policies. Their nostalgic longing for the mythic "golden age" of the protective national state also makes them deeply skeptical of transnational projects such as the EU.

F. Their obsession with national sovereignty also means that populist parties have few convincing solutions to 21st century challenges. Many of these are intrinsically transnational in character, such as coping with climate change, migration, economic development, scientific and technological progress; and regional and global stability. None of these objectives can be achieved by pulling up the drawbridge and withdrawing to behind fences or walls. All require an open mind and international engagement and cooperation.

Many consider the 2008 financial crisis and migration flows as key to the rise of European populist parties. What factors do you attribute it to?

It is useful to differentiate between long-term factors and triggers or catalysts. Among the first, I would count a fairly broad rejection of globalization in the U.S. and in Europe by population groups suffering from stagnating incomes, job losses, and social insecurity who are angry about rising inequality and who believe that their children will have worse lives than they have. Another long-term factor is the crisis of representative democracy. For a number of reasons the bonds between the public and their political representatives have weakened. Many people have lost trust in mainstream politics and have turned to alternative political offers.

The 2008 financial crisis and the refugee crisis of 2015/16 acted as catalysts; they spread a sense of insecurity and loss of control that galvanized the already-present frustration and fueled the rise of populist parties.

How do you read the outcome of the Dutch parliamentary elections? Is it a sign that the populist upsurge has been stopped? Last year, Austria's far-right presidential candidate Norbert Hofer was defeated by rival candidate Alexander Van der Bellen. How do you think the defeat will affect the populist movement in Austria?

After the double-shocks of the Brexit vote and the election of Donald Trump, a domino theory developed, according to which one European democracy after the other would succumb to the onslaught of the populist right. This approach was always implausible as the political dynamics but also the electoral and constitutional rules vary greatly from country to country.

In view of the proportional electoral system in the Netherlands and the absence of potential coalition partners, Geert Wilders never had a realistic chance to lead the next Dutch government. Still, his unexpectedly weak performance and the success of Mark Rutte gave a psychological boost to the mainstream parties in Europe. Unfortunately, it is also true that Wilders' xenophobic and anti-European polemics managed to drive some of the mainstream parties in the Netherlands towards increasingly restrictive positions on migration and the EU.

As the Austrian president has no real power, this contest was primarily of symbolic relevance. Still, the victory of the "Green" candidate Van der Bellen over the rightist Norbert Hofer confirmed that one can win with a consistently pro-European liberal-democratic approach. However, Hofer's party is still popular in Austria and could do well in the Austrian parliament elections which will take place in October 2018.

What is your opinion of European populist parties that are currently in power (e.g., in Hungary)? How sustainable do you think their administrations and support are?

Populist parties are now in government in several

> ...it is wrong to believe that the current wave of populism would simply sweep away the existing political order of Europe.

EU member states, even though apart from Poland and Hungary, they are junior partners in coalitions. Experiences vary. Sometimes joining a coalition will prompt a populist party to turn more mainstream and responsible. This, for instance, happened to the Greens in the 1980s and 90s. Sometimes it has led to a massive drop of support for such parties when the protest voters turn elsewhere. This seems the case in Finland, where according to the polls the True Finns have lost much of their appeal. The situation is, of course, different when a populist party dominates the government. In such cases, we have seen a rise of nationalist rhetoric and worrying tendencies to curtail constitutional checks and balances, and the freedom of media.

Has the rise of right-wing anti-EU populism had any effect on the EU's abilities to perform its duties?

The EU institutions are still dominated by mainstream parties from the centre right and the centre left. About 25 percent of the members of the European Parliament belong to populist parties but they are mostly marginalized in the decision-making process. The direct effect of the rise of populism is therefore quite limited, but the indirect effect is significant. Fear of their populist competitors prompts mainstream politicians to prioritize national interests and adopt EU-skeptical positions, which weakens solidarity among member states and makes progress towards European solutions more difficult. Populist parties are also at least partly responsible for the growing demand for referenda on EU matters, which for them are perfect instruments for mobilization. Recent experience with referenda in Greece, Denmark, the Netherlands and the UK has shown how difficult it is to win such referenda in the current political climate. Fear of further defeats has crippled the EU's ability to adopt significant reforms.

In the U.S., populist campaigns utilized social media and other digital means to help spread and reinforce their messages. Do you think this strategy is, or can be, effectively used in European populist campaigns?

Also in Europe, many populist movements are savvy and successful at using social media, leaving most mainstream parties far behind. The speed, superficiality and interactive nature of social media make them very well suited to spread populist ideas. The fragmentation of the information space into "bubbles" within which people mostly listen to ideas that they already hold, greatly favors the work of populists. Phenomena like "post-truth" and "fake news" present huge challenges to traditional representative democracy. So far nobody has come up with a convincing response.

The 2017 elections in France and the Netherlands included populist candidates. Other populist parties also exist across Europe. What do you foresee for the possible expansion and success of populist movements in Europe?

The national elections in European countries in 2017 are clearly of major importance. But it was wrong to believe that the current wave of populism would simply sweep away the existing political order of Europe. And it would be equally wrong to assume that after Geert Wilders modest results, the convincing victory of Macron over Le Pen, and the likely defeat of "Alternative fuer Deutschland" in Germany, the populist threat would disappear. As long as the main underlying reasons for the alienation of large parts of Western societies, the anger of the losers from globalization and the frustration with traditional democratic politics are not addressed, the challenge will remain.

What can be done by the EU to assuage fears of those supporting right-wing populist parties in Europe and therefore, lessen support for those groups?

The EU and its member states have to pay more attention to the consequences of inequality and social injustice, and take action to cushion the effects of global competition and asymmetric shocks on vulnerable citizens. Apart from providing opportunities and assistance to these people, the EU also needs to tackle inequality by promoting fairer tax systems that ensure multinationals pay their fair share, exposing tax havens, and preventing money laundering and corruption.

Managing migration well is another crucial challenge. Europe needs immigration in view of its demographic decline, but the process needs to be handled in an orderly manner. This requires better control over the external border, better common rules in the areas of migration and asylum, and more effective institutions.

Concrete results in areas of direct concerns to the citizens are obviously the best way to regain their trust and defeat the populist. But EU institutions and the governments of member state should also explore new ways to make politics more transparent, participative, and democratic. If citizens felt more involved and consulted, they would regain confidence in their representatives and would be less attracted by the simplistic solutions of populist parties.

Stefan Lehne is Visiting Scholar at Carnegie Europe, Lecturer at the Diplomatic Academy Vienna. His main research interests are: European integration, EU foreign policy, and migration. He has also been Director General for Political Affairs, Austrian Foreign Ministry Vienna and Director for the Western Balkans and Eastern Europe in the EU Council Secretariat, Brussels.

The Current State of Right-Wing Populist Parties in Germany

Interview with Professor Fabian Vichow
University of Applied Sciences, Düsseldorf

What is the current state of right-wing populist parties in Germany?

There were several attempts over the last 20 years to establish a right-wing populist party in Germany. Yet, none of the attempts were successful. However, in contrast to preceding failures, the Alternative for Germany party (Alternative für Deutschland/AfD) founded on February 6, 2013, has been quite successful from the very beginning. The party almost missed entry into the Bundestag in autumn 2013 but with its 25,000 members as of January 2017, it has sent elected delegates to thirteen regional parliaments. The share of votes was between 5.5 percent in the city-state Bremen and 24.3 percent in Saxony-Anhalt. Due to the success of the AfD, smaller right-wing populist parties such as The Freedom party (Die Freiheit) or the Pro Germany party (pro Deutschland) have decided to dissolve or not to participate in elections. Thus, the AfD has also become a magnet for activists of several right wing groups and networks.

Do you see any striking similarities between German populist parties and other major European populist parties?

The history of the AfD is different from the Austrian Freedom Party or the French Front National party, both of which have deep roots in the extreme right of their particular country. The AfD is also different from the right-wing populist parties in Denmark and Norway, which started as anti-tax parties several decades ago. Yet, most of the right-wing populist parties in Europe share some basic ideas, which include: a strong anti-immigrant position (especially regarding refugees from non-European countries), a nationalist economic and cultural agenda, the approval of traditional heterosexual family and gender arrangements, and the rejection of the European Union while favoring the idea of strengthening sovereign statehood instead of the integration of states into international alliances and agreements. Another relevant position is the producerist formula which places blame on particular groups for taking advantage of work done by the majority. In the German context, this has been used to rebuke the Greeks, and in others contexts such disdain has been directed against Romani people, Jewish populations, and the homeless. Yet, in recent years, there has been a shift toward a tougher anti-Islam position so parties such as the Front National have tried to present themselves in favor of Judaism and Israel. However, in the AfD, openly anti-Semitic positions are even held by members of parliament.

The political situation and the political culture in European countries vary from country to country, making it difficult to compare right-wing populist groups. In countries like Poland, religion plays a prominent role to explain the success of right-wing parties. In many others countries, right-wing political parties have made a profit in recent years because voters were disappointed by the political agenda of conservative and social democratic

Although it had a significant focus on the Eurozone crisis in the beginning, the [AfD] party was never a single-issue project.

parties and turned off by the behavior of party leadership. In addition, all right-wing populist parties that could make the strongest break-ins in the electorate of the traditional democratic parties portray themselves as the political force that dares to speak about societal developments and problems about which other political actors and the mainstream media allegedly do not talk. In line with this, parties like the PVV in the Netherlands, the UKIP in Great Britain, and the AfD present themselves as anti-establishment actors.

Your research has included analysis of the right-wing group, Alternative for Deutschland (AfD). How has this group evolved?

The story of the AfD can be told from different starting points. One is a book published in 2010 written by Thilo Sarrazin. Although a member of the Social Democratic Party of Germany, his book – titled *Germany Abolishes Itself* – is a racist narrative that links the decay of Germany to immigration and multiculturalism. In a way, its argument is similar to that of U.S. authors Charles Murray and Richard Herrnstein in *The Bell Curve*. As a non-fictional book, Sarrazin's deed was sold more than 1.6 million times. Tabloid media also heavily popularized its main ideas. In late 2010, a survey showed that 18 percent would vote for a notional Sarrazin party. A second starting point are the many surveys conducted over the last 15 years which clearly show that there is a relevant minority amongst the German population that holds anti-immigrant, anti-Muslim, and nativist attitudes. Although these two issues are not directly linked to the party history, they have been clear indicators that there was the potential for a right-wing populist party in Germany too.

A third starting point is the foundation of the party itself and its evolvement in the narrow sense. In September 2012 Bernd Lucke, a professor in economics, Alexander Gauland, a former newspaper editor and State Secretary in Hesse, and Konrad Adam, a former editor of the renowned daily Frankfurter Allgemeine Zeitung founded the political group Electoral Alternative 2013 (Wahlalternative 2013 on). With its opposition toward German federal policies concerning the Eurozone crisis, this group later formed the cornerstone for the AfD. The party's leading representatives were quickly invited to TV talk shows and got wide media coverage – not least due to the high proportion of academics in their ranks.

Although it had a significant focus on the Eurozone crisis in the beginning, the party was never a single-issue project. From the beginning, issues such as anti-immigration and traditional family and partnership models played a significant role. The rapid success in elections – in May 2014 the party won seven seats in the European Parliament election – made the party attractive for different political milieus. Thus, activists from a neoliberal milieu, from national-conservative milieus, and from right-wing populist to extreme right milieus tried to broaden their influence in the party.

A first breaking point had been the party convention in July 2015 when, after months of internal infighting, party leader Bernd Lucke was expelled from the party. This marked a decisive trend further to the right actively promoted by a coalition of forces around Frauke Petry head of the Saxon branch of the AfD on the one hand and Björn Höcke head of the AfD in Thuringia on the other hand. While Frauke Petry and Jörg Meuthen (who was considered moderate for a long time) took over the party leadership, internal fighting did not come to an end. With further electoral successes and the next national elections approaching, rivalry between individuals and competition of different political concepts perpetuated the infighting. The party congress in April weakened the position of Frauke Petry substantially and gave male bonding of Jörg Meuthen, Björn Höcke, and Alexander Gauland the upper hand.

From the beginning of 2016, polls had seen the AfD at more than ten percent for the national elections in September 2017. Yet, recent surveys had noticed a decline in support down to seven or eight percent. This would still allow the AfD to enter the Bundestag, but many in the party are getting nervous about a further decline in voter support. Simply speaking, the infight is between one approach that seeks to enter into a coalition with the Christian Democratic party once Angela Merkel has stepped back, and a second approach which argues for the AfD as a political force fundamentally in opposition to the democratic parties.

In fact, the party was able to garner a stable base of voters of some 4-5 percent in a quite a short period. Amongst them, a growing part have a working class background or are unemployed. Support in East German areas is above average, and many who have voted for extreme right parties before are now dedicated to the AfD as their project.

Did the outcome of the U.S. presidential election and/or Brexit have any impact on AfD's campaigns?

As I see it, the U.S. election did not have a big impact on the decisions of voters but it did bolster the confidence of the extreme right in general and the AfD in particular. In their eyes, the Brexit decision and Trump's victory prove that a nationalist and nativist agenda can be fought and won against the majority liberal establishment. Besides their own victories in elections since 2014, this is what gives them confidence that they might soon be successful on the national level too.

What effect, if any, has the AfD party had on other German parties in their campaigns? And what effect has it had on the German government in general?

That is a complicated issue as it is not always easy to identify what drives a particular political decision and to isolate the most important factor(s) in a particular decision-making process. The biggest factor impacting German politics is the influx of a huge number of refugees in 2015. While German Chancellor Angela Merkel did not retreat from her famous statement "We will do it", the government over which she presides has put several regulations in place to drastically reduce the number of refugees coming into Europe in general and to Germany in particular and by which an increase in deporting refugees whose application for asylum had been denied should be secured. Even the deportation of asylum seekers from Afghanistan back into that war-shaken country has been implemented. These decisions are probably made in part to show (potential) AfD voters that the government is not running a laissez-faire policy in the fields of migration, asylum, and security. But it also plays a role that the traditional idea of an ethnically homogenous German people whose identity will be damaged by a growing number of immigrants is still alive and strong amongst the leaders and rank and file of the parties currently in the national parliament. There are some examples in which the wording of representatives of the Left party and the Social Democratic party hardly differed from what was said in AfD statements. Of course, these parties at the same time emphasize that the AfD positions are often racist and derogatory.

How effective have German right-wing populist parties been to engage participation from previous non-voters to become active?

Again, this effect is only relevant for the AfD. In fact, in most of the elections in which the AfD ran successfully it was able to bring voters to the ballot box in significant numbers who had not voted in the elections before. Unfortunately, there is hardly any empirical data about the participation and voting decisions in the penultimate elections. This would better clarify, if someone who, for example, had voted for the Social Democratic Party in the 2000s did not vote in the early 2010s and now turns out as an AfD voter.

How have German populist movements embraced digital media (e.g., social media, bloggers) to advance their causes?

The AfD is running a huge number of websites and is using different digital media formats. Facebook is quite successfully used by party chairwoman Frauke Petry who has the greatest number of followers of all AfD leaders and makes use of it in order to enhance her position in the internal rivalry. Yet, in order to reach out for a broader audience party leaders follow a tactic of provocation. They come out with a radical or offensive statement that is multiplied by the mass media. When there is heavy criticism they often claim a misunderstanding or being quoted in a wrong way. In doing so, they reach out to different audiences – the radical right wing and the more conservative.

Fabian Virchow is Professor of Social Theory at the University of Applied Sciences in Düsseldorf, Germany, where he also acts as the director of the Research Unit on Right-Wing Extremism.

The Role of Media in Populist Movements

Interview with Dr. Sven Engesser
University of Zurich, IPMZ (Institute of Mass Communication and Media Research)

You've performed research about populism and media with several colleagues through the European Cooperation in Science and Technology (COST). What was the goal of the research?

COST primarily is a networking tool. Our specific COST action, entitled "Populist Political Communication in Europe," spans 32 countries. It investigates how political actors employ populist communication strategies, how populism manifests itself in the media, and how populist messages affect citizens. As a first step, we published an edited volume that gathers literature reviews on populist communications from 24 countries. We determine the prevalence of populism in the media content by analyzing migration news and journalistic commentary. Simultaneously, we are conducting experiments in order to find out how populist messages affect populist attitudes. These two projects will be complemented by in-depth interviews with politicians and journalists about their motives and aims related to populist communication. In this way, we cover the entire process of communication, from the communicators over the media content to the recipients. As a result, we hope to provide public actors with recommendations on how to deal with populism. At the same time, I am involved in a so-called National Center of Competence in Research (NCCR) at the University of Zurich, which is also partly dedicated to media populism. We combine content analyses of the media coverage with surveys among media users in order to analyze the effects of populism under real-life conditions. Additionally, we investigate how politicians present themselves in talk shows and social media.

What are some key highlights of the group's findings?

We can confirm that populism is on the rise throughout Europe. The ideological spectrum ranges from left-wing populism (e.g., Syriza in Greece) to centrist populism (e.g., Yesh Atid in Israel) to right-wing populism (e.g., National Front in France). In general, left-wing populists attack the economic elites, centrist populists claim to represent the middle class, and right-wing

Although populism has a "chameleonic nature" (as political scholar Paul Taggart puts it) and adapts to the local context, we were able to identify some favorable conditions: economic crises (predominantly in Southern Europe), migration (predominantly in Western Europe), ethnic conflicts (predominantly in Eastern Europe), political distrust, and a supportive media environment.

populists target migrants or ethnic minorities. Although populism has a "chameleonic nature" (as political scholar Paul Taggart puts it) and adapts to the local context, we were able to identify some favorable conditions: economic crises (predominantly in Southern Europe), migration (predominantly in Western Europe), ethnic conflicts (predominantly in Eastern Europe), political distrust, and a supportive media environment.

We have also come up with some analytical clarifications with regard to media populism. We distinguish populism by the media, populism through the media, and populist citizen journalism. The first type refers to media organizations and journalists who assume the role of populist actors themselves (e.g., Breitbart). In contrast, the second type implies media organizations that consciously or unconsciously disseminate populist messages because the media and the populists share the same goals, such as attracting the attention of mass audiences (e.g., BuzzFeed). The third type occurs when populist messages from the citizens enter the public sphere through blogs and reader comments.

At the NCCR, we found that populism in the press is more prevalent in authoritarian cultures, weekly magazines, and opinion pieces. We also showed that fringe parties use more populism in social media than mainstream parties.

What populist groups have utilized media most effectively in their campaigns to attract and sustain followers? How have they done so?

In general, populists have an ambivalent relation to the media. On the one hand, the media offer them a direct linkage to the people. On the other hand, they regard the established mass media as part of the elite. A populist actor who instrumentalizes the media in a very professional way is the Swiss People's Party. It issues two official party papers, and two weekly newspapers that are both edited by parliamentarians of the party. Further, the founding father of the party entertains a weekly videocast. Finally, the party successfully draws on the complete repertoire of mass media in its referendum campaigns which are a constant element of Swiss direct democracy.

What about those groups that have most effectively embraced the use of digital media?

Social media provide the populists with even more suitable means to circumvent elite actors than the established mass media. Two textbook examples for Internet-savvy populists are Beppe Grillo in Italy, and Geert Wilders in the Netherlands. Both shun the established mainstream media. They only give interviews to benevolent or foreign media organizations, such as Russia Today. Grillo and Wilders also very actively communicate through social media, preferably Twitter. In this regard, they can be regarded as predecessors of U.S. President Donald Trump.

Where populist parties are in power, have any media control measures been taken by the government?

In Europe, there have not been many cases of populist politicians coming into office so far. A good example, however, is Hungary, where the populist Prime Minister Viktor Orbán has introduced a strict media policy. He has established the National Media and Communications Authority (NMHH) and has equipped it with extensive competencies. He has also unified all public service broadcasters under a single umbrella organization (MTVA). This behavior has drawn Orbán into an ongoing conflict with the European Union. There are also several cases in Latin America where populist politicians employed harsh media regulations after they had become Presidents, such as Hugo Chavez in Venezuela.

Some consider the overall impact of digital media in political campaigns to be overblown. For example, that Facebook users aren't inclined to change their opinions in spite of campaign posts and even fake news. What are your thoughts?

In my opinion, this notion becomes increasingly obsolete. Findings from the Pew Research Center show that the relative majority of young adults (roughly a third) in the U.S. named social media as their most helpful source of information for learning about the 2016 presidential election. According to Oxford University's Reuters Digital News Report, almost two thirds of the young adults across 26 countries indicated online media as their main source of news. We also know from our own studies at the NCCR that populist media content may affect populist attitudes and even lead to an increased polarization of society.

What role should participatory journalism have in today's media?

Participatory journalism may fulfill at least three main functions: First, it may complement the professional journalism by filling existing gaps in the media landscape and covering marginalized subjects. Second, it may serve as a corrective for the professional journalism by pointing to the latter's deficits in terms of authenticity, credibility, and transparency. Third, it may provide the citizens with a low-threshold environment for social participation.

What have you found to be the largest challenge(s) in performing research on populism and media?

It is crucial that the term "populism" increases and maintains its analytical clarity. We argue that populism can be defined as a small set of ideas that is based on the fundamental antagonism between the people, on the one hand, and the elite or "others," on the other hand. In this way, it can be distinguished from similar concepts such as agitation, nationalism, xenophobia, sensationalism, and opportunism. Not all scholars have to share this understanding, but they should provide explicit definitions of their own when operating with the term "populism." Otherwise, it risks trailing off into ambiguity.

Dr. Sven Engesser is Senior research and teaching associate at the Institute of Mass Communication and Media Research, University of Zurich. Dr. Engesser is also a Member of the Management Committee of COST Action IS1308 on "Populist Political Communication in Europe". Previously, he was research and teaching assistant at the Department of Communication Science and Media Research (IfKW) at LMU Munich. Dr. Engesser has co-edited a special issue of *Information, Communication & Society* on "Populist Online Communication" that will be pusblished in September 2017.

Populism in the U.S.A.: a first-hand account of its changing nature from the 1960s

Interview with Professor Harry C. Boyte
Augsburg College

You became exposed to populism early in your life. Would you share that experience and how it shaped your thoughts about populism?

I grew up in the South, in Atlanta. My father, who had a Southern background, was manager of the Atlanta Red Cross, and had been a newspaper reporter during the Great Depression. He had pro-integration views, very rare in his world. He got involved in school desegregation and then went to work for Martin Luther King on the executive committee of the Southern Christian Leadership Conference (SCLC) in 1963, just before the March on Washington. He was the only white on the board and brought an important understanding about Southern white mentality.

I worked as a field secretary for SCLC as a young man. The experience was formative in several ways. First, the citizenship education program deeply shaped my views of education. The program grew out of folk school and popular education traditions which ground education in the cultural life of communities and belief in the enormous untapped talents of everyday people. Citizenship schools formed an invisible dimension of the movement in today's public memory, but they were enormously important in reality. Eight hundred citizenship schools across the South educated thirty thousand grassroots leaders in literacy and skills of empowerment, teaching people how to make constructive change in their communities. The citizenship education gave the whole movement a populist quality, populism as deep belief in everyday people's talent and intelligence, whatever their formal schooling. Citizenship schools were founded in the conviction that wisdom could be found in low income African American communities in rural communities as well as in cities.

In addition to skills of making change, the citizenship schools taught nonviolent philosophy. This was not pacifism, the refusal to use violence under any circumstances – a distinction King got from Reinhold Niebuhr. It also wasn't a tactic, although movement organizers saw the strategic and tactical uses of nonviolence. Nonviolence in the movement was most importantly a philosophy of human interaction. It involved the refusal to demonize opponents, a political and public disciplining that meant you learned to have goodwill towards your enemies and didn't seek to humiliate them. This stance involves mental, spiritual, and moral habits that are not easy to learn. One has to learn the disciplines. For instance, in the nonviolence training across the South, a central question was what do you do when if you are subject to abuse, not only physical, but verbal? How do you respond with boldness and power, not with defensiveness or meekness -- but also not with violence?

The process of civic and nonviolent education generated a widespread schooling across the South in what I would call a different kind of politics.

King assigned me to work with low income white communities, which was very useful in understanding the immense complexity of any community. People are complicated. Communities have democratic resources one can build, as well as prejudices and parochialisms. King's assignment came learning brought about an experience I had in St. Augustine Florida with the Klu Klux Klan.

One day I went out to the Old Jail as I was worried about a friend who had been arrested in a demonstration — the brutality that the jailors displayed toward civil rights demonstrators was a regular topic of conversation among SCLC staff members. Many were held without water all day long, packed outside the building in a wire enclosure called "the pen." The hot Florida sun beat down relentlessly. Some passed out.

I talked to Cathy, my friend through the bars. She was fine. But when I came back to the car five men and a woman suddenly surrounded me. I realized that they must have followed me out from town. One said, "You're a goddamn Yankee communist. We're going to get you, boy."
I took a breath. Then my southern roots flooded back. I said, "I'm a Christian and the Bible says love your neighbor.' I love blacks, like I love whites. But I'm not a Yankee. My family has been in the South since before the Revolution. And I'm not a communist." Searching for a word to describe my confused identity — and remembering an occasional remark of my father — I tried on a different label. "I'm a populist," I said. "I believe that blacks and poor whites should get together and do something about the big shots who keep us divided and held down." There was silence. The group looked at an older man, dressed in coveralls, wearing a straw hat, to see what he would say. He scratched his head.

"There may be something in that," he said. "I don't know whether I'm a populist. But I read about it. I ain't stupid. The big shots do look down on us. The mayor will congratulate us for beating you up. But he'd never talk to me on the street."

He continued, "I ain't a Christian myself. I'm a Hinduist. I believe in the caste system." For a few minutes, we talked about what an interracial populist movement might look like. Then I drove quickly back into town.

Several days later the Klan held a march in front of the Southern Christian Leadership Conference office in the African-American part of town. That summer was a battle of flags. Civil rights demonstrators marched under the American flag. The Klan countered with the Confederate flag.

I was standing with the crowd in front of the office, perhaps the only white in the group. Dr. King was nearby. The Klan philosopher, in the front row of their march, saw me and waved. I gave a tepid response, trying to be inconspicuous. But King saw my gesture. He asked me what that was all about. I told him the story.

King said, "I've always identified with populism. That was a time when Negroes and whites found common ground." I had only a vague sense of what he meant — the term, populist, had floated to my consciousness like a rescue raft.

I didn't know it then, but I realize he must have known the history of populism in the south. The original movement to go by the name "Populist" was formed in the 1880s and 1890s among black and white farmers in the South and Midwest. It was not first an electoral movement – its base was an enormous network of cooperatives which farmers organized in efforts to free themselves from bondage to the merchants and the banks. For a time, the movement included interracial alliances, shaky though they were, that defied racial taboos. King's political mentors like Bayard Rustin and A. Philip Randolph were also involved in

Populism in any form speaks to the unsettling of civic, political, and cultural relationships.

the second great wave of populist and interracial organizing of the 1930s. I'm sure they conveyed that history.

This experience shaped how I thought about populism but I didn't start theorizing populism as a different politics until the late 1970s and early 1980s.

Moving ahead to more recent times, what do you see triggering the resurgence of populism in the United States, on both sides, left and right?

I would say there is populism with three sides. Right, left, and what I call civic populism. This is the tradition I identify with. It's beyond partisan ideology. I wrote about moments and movements which expressed such populism, which I also called citizen politics, in *Commonwealth: A Return to Citizen Politics*, the book that got us started at the Humphrey Institute of Public Affairs in the late 1980s.

Several things are at work in the rise of any kind of populism. Analysts talk about the global economy and social dislocation, but the diagnosis usually misses social fragmentation and atomization that's going on with the rise of individualism. Populism in any form speaks to the unsettling of civic, political, and cultural relationships. Another element is the feeling of people being left behind economically. Elites, both corporate and governmental, seem out of control.

Let's go back to your work with the civic populism. Would you expand on your experience?

Theoretically and journalistically in the '70s, I began to write about citizen action growing out of the 1960s, what had happened to the movement impulse. My views about populism changed over time.

First I began to realize that the progressive or the left framework was detached from the historical and symbolic language of American democratic traditions. Its language was about rights and resources, not meanings and narratives. Here I was theorizing what I had seen as so powerful in the civil rights movement. In the 1970s, I helped to create an organization, the New American Movement, whose mission was to bring the student movements of the late '60s "back to America." I didn't have a theoretical language besides democratic socialism and worked to unite the New American Movement with Michael Harrington's group, called the Democratic Socialist Organizing Committee.

I wrote about community organizations forming across racial and cultural lines, as well as other kinds of citizen action starting with my first book, *The Backyard Revolution*, in 1980. I became convinced that there was an indigenous civic democratic tradition in America, focused on civic autonomy, associational life, and the public meanings and values of work. This tradition understood the commonwealth not only as popular government, republican government, but also as solving public problems and creating and sustaining libraries and schools, community centers and parks, bridges and roads, the commonwealth of common goods. The tradition generated a populism that was cross partisan, not ideological. It answered Sombart's famous question from 1906, *Why is there no socialism in America?*, differently than generations of American intellectuals. Rather than exploring "what's wrong" with America, a focus on civic autonomy illuminated the presence of an alternative politics different than partisan politics and state-centered understandings of democracy. In *Commonwealth*, I presented the argument that the erosion of citizen politics was not only because of the spread of marketplace categories, but also of the spread of technocratic modes of thinking through professional systems. People were turned into clients and customers. What had once been civic sites like schools, congregations, ethnic organizations, and locally rooted trade unions and businesses, were changing their internal character, becoming service delivery operations. A significant factor was the way professionals became trained in narrow, disciplinary identities. The older sense of civic professionalism, work involving collaboration with lay citizens to build the civic life of communities, shifted. Professional identities shifted from civic to disciplinary.

Then I began to realize another problem. Citizen campaigns and elections were being shaped by mobilizing technologies with a specific and seldom discussed formula which I would call a Manichean model. Let me describe it.

In 1974, the environmental group called Citizens for a Better Environment developed the door-to-door canvas. It involved paid staff going door to door to raise money and get signatures around an issue. The Midwest Academy, which I was working with, became the main center for spreading that method. The context was the large-scale corporate mobilization and its agenda, visible in groups like Business Roundtable. *Business Week* wrote in 1974 that how people had to get ready for the new reality is that the country has to have redistribution upwards. This meant in practical policy terms that there was a significant effort to roll back environmental, consumer, affirmative action, and progressive tax legislation from the 1960s. That was very clear from the '72 election, and John Connolly had a front-page interview in the *Wall Street Journal* describing that agenda. The canvas was developed in part to kind of push back on a large scale.

A lot of people bought into that kind of anti-corporate populism out of the progressive side. I wrote a book with Steve Max and Heather Booth, founder of the Midwest Academy in 1986, *Citizen Action and the New American Populism,* to defend the canvass. But shortly after I became convinced that the formula which made the canvass work had bad effects on canvassers – an enormous number burnt out, many became cynical. And it also eroded the larger bonds of citizenship. In the formula there is always an enemy, one defines issues in good versus evil terms, one figures out how to frame them in ways that have broad appeal, and one figures out how to appeal people's sense of victimization. Scripts inflame people's emotions. I'd call this a Manichean political framework. It was successful in the '80s, in widespread citizen campaigns such as natural gas taxes and winning passage of toxic waste legislation. But it had the unintended consequence of contributing to the polarization of political language. Of course, conservatives picked it up, too. It came to shape talk radio, internet mobizations, and political campaigns. The Tea Party used Saul Alinsky's book, *Rules for Radicals*, as a primer in polarizing populist tactics. In the 2016 election, both Trump and Clinton used versions of the same formula. So did Bernie Sanders, although he had a larger ideological appeal that didn't demonize Trump supporters in the same way Clinton did.

So people think of populism as either right wing or left wing. But populism in its richest, oldest sense is not about beating up on the evil other, it's actually about citizens claiming responsibility for the civil life of communities, and the larger democratic project, challenging unaccountable power but also advancing a constructive alternative. The civic roots of populism, placed in sites and local schools and ethnic groups, community groups, businesses, locally grounded unions, and neighborhood networks, still exist but they are not the center of the action when people think of populism.

With the expansion of digital communication and media, how is this affecting populist movements, if at all?

Social media and more broadly the digital revolution are here to stay. In fact, the digital revolution is expanding at an exponential rate. Nine computer and artificial intelligence scientists just made a very powerful case about this in a recent article in *Scientific American* called, *Will Democracy Survive Big Data and Artificial Intelligence?* It shows that the algorithms in the digital revolution enhance capacities for the manipulation of people around polarizing mindsets and the fragmentation. They can inflame opinion, demonize whole groups and swaths of the population, create abstractions, and manufacture political identities. It's like the McDonalization of society. Here, a different kind of civic populism becomes crucial for bringing back the nonviolent philosophy where one focuses on relationships, not simply issues. You don't demonize your enemies or your opponents. This kind of populism is crucial as a counterweight to the algorithms which otherwise fragment and polarize. I'm wondering how do we develop a civic populist and nonviolent counterweight to the Manichean demonization that's taking place?

We have to figure out how to bring an alternative civic populism to scale. There are a lot of digital uses that help that, including the work done during the Obama campaign in 2008. In our training, we had people learn how McCain supporters are not your enemies by using organizing practices, like the idea of public narrative, everybody has a story, everyone is complicated. You can't put people in boxes. That was large scale training. Another campaign which built around that was Minnesotans United for All Families, which opposed a constitutional amendment to ban gay marriages. For the first time after 30 fights which had used a mobilizing, demonizing approach, the Minnesotans United campaign asked people why they had questions. They developed a much more cultural, narrative message: marriage is so valuable that it needed strengthening and reinforcing, and everyone should be involved. The campaign also generated more than a million conversations in the state around storytelling, people's personal histories, asking questions, and having conversations.

That is what I would call a civic populist methodology, taken to scale and built around relationships, not demonizing. It's counter to the Manichean mobilizing mindset. Even though it was very successful, as was the Obama 2008 campaign, it's interesting that it's not evoked in discussions of *evidence based* campaigns. People don't really mean *evidence based*; they mean, "we have our technocratic framework, and this was what we are convinced works."

The distinction between a civic populist and an ideological populist approach is that ideological populism uses technologies to substitute for relational interactions. This is the substitution of information for relational. There are forces pushing back. An important way to understand Pope Francis's populism is in these civic populist terms. His climate encyclical, *Laudato Sí*, has a brilliant critique of technocracy and substitution of information for relational.

Civic populism reinserts, reaffirms, and recontextualizes the informational in the relational.

Harry C. Boyte is founder of the Center for Democracy and Citizenship at the Humphrey School of Public Affairs, now merged into the Sabo Center for Democracy and Citizenship at Augsburg College where he now serves as Senior Scholar in Public Work Philosophy. He is also a Senior Fellow at the University of Minnesota's Humphrey School of Public Affairs.

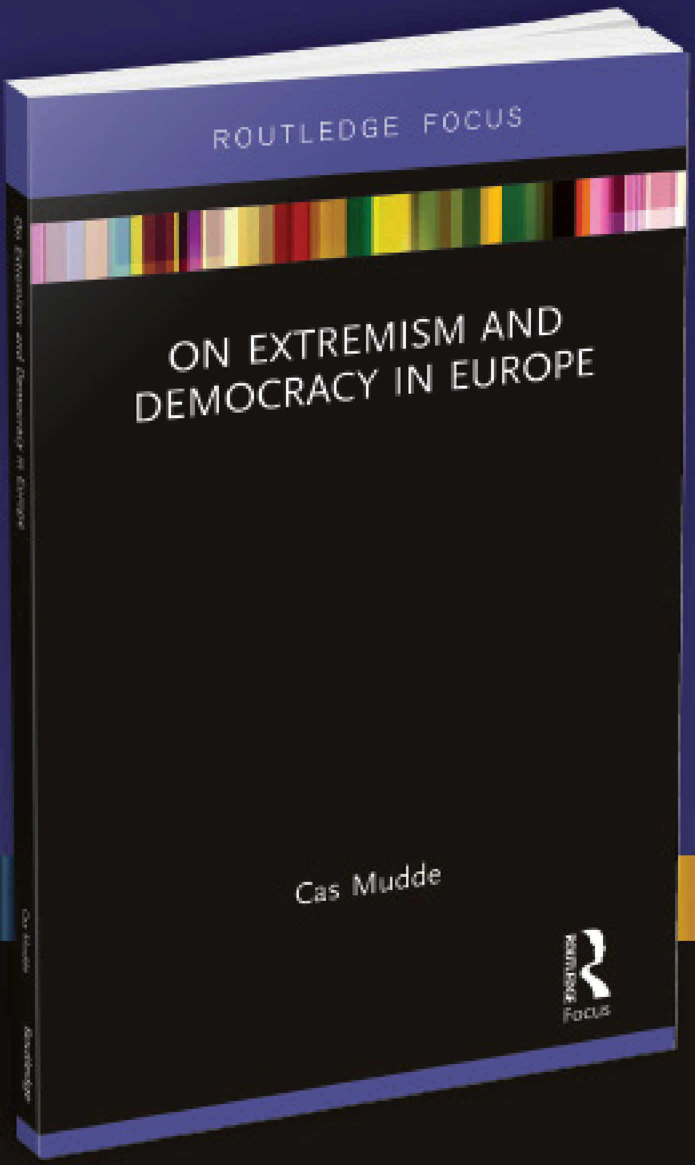
In 2012 he served as Coordinator of the American Commonwealth Partnership, a coalition of higher education groups and institutions created on invitation of the White House Office of Public Engagement which worked with the Department of Education to develop strategies to strengthen higher education as a public good in the anniversary year of the Morrill Act, creating land grant colleges. From 1993 to 1995 Boyte was National Coordinator of the New Citizenship, a cross partisan alliance of educational, civic, business and philanthropic civic groups, which worked with the White House Domestic Policy Council in the Clinton administration to analyze the gap between citizens and government and to propose solutions. Boyte presented its finding to a Camp David summit on the future of democracy in 1995 with President Clinton and other senior members of the administration which helped to inform Clinton's 1995 State of the Union.

Boyte is an architect of the Center's public work framework for citizenship, an action-oriented civic agency approach which has gained international recognition for its theoretical innovations and practical effectiveness. Along with citizens as co-creators, public work is a core concepts in "Civic Studies," a transdisciplinary and international emerging field focused on agency and citizens as co-creators which Boyte co-founded in 2007. Boyte is also the founder of Public Achievement, an international civic education and civic empowerment initiative for young people now in hundreds of schools and communities in more than two dozen countries.

Boyte's edited volume, *Democracy's Education: Public Work, Citizenship, and the Future of Colleges and Universities*, a collection of essays by leading university presidents, policy makers, faculty, students, community organizers and public intellectuals on how educators can be agents of change not objects of change, was published by Vanderbilt University Press, 2015.

Boyte has authored nine other books on democracy, citizenship, and community organizing including *Everyday Politics* (PennPress, 2004); *Building America* (Temple University Press, 1996) *Free Spaces*, with Sara Evans (Harper & Row, 1986; University of Chicago, 1992); *CommonWealth* (Free Press, 1989); and The Backyard Revolution (Temple, 1980). His work has appeared in more than 150 publications including *Education Week*, where he writes a weekly blog, *Political Theory, Policy Review, Public Administration Review, Nation, New York Times, Wall Street Journal, Los Angeles Times, Christian Science Monitor, Business Day* (South Africa), *Change, Perspectives on Politics, democracy, Kettering Review*, and *The Journal of African Political Science*. His political commentary has appeared on CBS Evening and Morning News and National Public Radio.

In the 1960s, Boyte was a Field Secretary for the Southern Christian Leadership Conference, the organization headed by Dr. Martin Luther King, Jr., and subsequently was a community and labor organizer in the South. His Ph.D. is in social and political thought from the Union Institute. Harry Boyte is married to the South African democracy educator Marie Louise Ström. He lives part of the year in Johannesburg, South Africa.


ROUTLEDGE FOCUS
ON EXTREMISM AND DEMOCRACY IN EUROPE
Cas Mudde
Focus

Tracing the Transformation of Populism in Europe and America

Interview with Professor John Abromeit
SUNY, Buffalo State

What are the historical roots of populism in the United States?

I'm not a historian of the United States, but in my own recent research on the historical roots of populism in Europe I have explored the transformation – from left to right – of the ideology of "producers and parasites" as one key element of the emergence of right-wing populist movements in Europe in the late nineteenth and early twentieth centuries.[1] In the European context this ideology first emerged during the French Revolution – for example, in the highly influential pamphlet "What is the Third Estate?" written by the Abbe Sieyes[2] – as a critique of the "parasitic" aristocracy by the "productive" members of the "third estate," that is, the bourgeoisie, workers and peasants. If one traces the evolution of this ideology, however, through the nineteenth and into the twentieth century, one sees how it is appropriated by certain socialist intellectuals, such as Pierre-Joseph Proudhon and Georges Sorel in France, who recast the bourgeoisie as the "parasitic" class, and the workers as the virtuous producers. It's important to see that the ideology always has a strongly moralizing tone, which is one of the most important defining characteristics of populism in general. Populists everywhere present politics as struggle between the virtuous people and the immoral "enemies of the people."

What I found in my own research, however, is that in Western Europe, this type of populism was very often a "producerist populism" which defined the morality or immorality of particular members of society in terms of their "productivity." So, to pick up the historical thread, one can see this ideology moving from the left to the right in early twentieth century, with the emergence of new, radical right-wing nationalist and populist movements in France, Germany and Italy. These movements set the stage for the emergence of full-blown fascist movements in the 1920s. The reception of the socialist Georges Sorel's writings by fascist thinkers (including Mussolini himself) in all three of these countries during this time provides one very clear example of this shift of the ideology of producerist populism from the left to the right.[3] To give just one example from Germany, the Nazi made a distinction between "schaffendes" (productive) and "raffendes" (parasitic) capital. Large German industrialists belonged to the former group and "international (Jewish) finance capital" belonged to the latter. By making this distinction, the Nazis were able to offer a right-wing populist and nationalist alternative to the Marxist doctrine of class struggle, which posited an inherent conflict of interest between employers and workers. If large industrialists were in fact "productive," then they were on the same side as workers, and both stood in opposition to "parasitic" finance. So, it's easy to see how this right-wing populist ideology transformed the Jews – but also the British, as the other putative agent of international finance – into the "enemy of the German people."

What's also crucial to recognize in Nazi, fascist and right-wing populist ideology more generally, is that its leaders present themselves as saviors of the oppressed people. "The people" must put their faith in these leaders if they are to have any chance of eliminating the particular groups who are responsible for their suffering. Another crucial aspect of populist ideology – both historically and in the present – is that it personalizes political conflict. In other words, rather than viewing political conflict or social domination in abstract, conceptual terms, populists always insist that concrete groups are responsible and that only by neutralizing or eliminating these groups will it be possible to solve the problem. So, rather than making specific policy recommendations as a way to address social problems, populists call for the elimination of the "immoral" and/or parasitic "enemies of the people."

Based on my own fairly limited research on the historical origins of populism in the United States, I think it is fair to say that such forms of producerist populist ideology also played a very important role in the nineteenth and twentieth century and – I would argue – continue to play an important role, right down to the present. My own thinking on this issue has been influenced by the brilliant work of the U.S. labor and race historian, David Roediger. He develops a concept of "herrenvolk republicanism" to describe the emergence of racialized forms of (white) working-class consciousness in the United States in the early to mid-nineteenth century.[4] What's similar about the United States and France in the nineteenth century is the centrality of republican political ideals. Classical republicanism differs from classical liberalism in its much great emphasis on virtue and the duties of citizens to subordinate their own personal or selfish interests to the good of "the people" as a whole. One need not look any further than Rousseau's Social Contract to find a classical formulation of this idea. But here we can also see the affinities that exist between republicanism and populism. Both view politics in terms of a "friend-enemy" relationship between the virtuous people and its immoral enemies. And, to leap ahead a bit, one can also see how such notions of politics could also be rather easily appropriated for a radical right-wing populist political projects, such as fascism, which also insists upon the absolute primacy of "the people" over the individual and her selfish interests and desires. For both republicans and fascists, virtue is demonstrated precisely by one's willingness to sacrifice oneself for the "good of the whole." This ideology played a progressive historical role in the French Revolution, but one would be foolish to overlook its potential to be placed in the service of extremely regressive political forces, as it was under fascism.

But, I digress. To return to the United States context, Roediger argues that white working class identity took shape in the United States in the nineteenth century in opposition to the enslaved or – later – the emancipated, but still downtrodden, Black underclass. White workers came to see themselves as independent, hard-working, self-disciplined, virtuous producers in contrast to the dependent, lazy, dissolute and immoral Black underclass. As Roediger also points out, this ideology of virtuous producers and immoral parasites targeted not only enslaved and/or poor Blacks, but could also – and often was – directed against upper-class "enemies" of the working class. In the U.S., as in Europe, there is a long history of anti-finance, which goes back at least as far as Andrew Jackson and his war against the Second Bank of the United States. Here, and later, in U.S. history, "parasitic" bankers were portrayed by progressive populists as the main source of the woes of the virtuous "common man," who earned a living by the sweat of his brow. Such anti-finance discourse was central, for example, to the populist "People's Party" of the 1890s. In the 1950s, when Joseph McCarthy provided the United States with a frightening example of the potential of right-wing populist rhetoric to mobilize popular opinion and create a "witch-hunt" atmosphere in the country, some historians and social scientist tried to trace McCarthy's rhetoric back to the progressive populists of the late 19th century. The most notable protagonist of this thesis – that the rhetoric of the progressive populists had been appropriated or even set the stage for a phenomenon like McCarthyism – was the eminent Columbia University historian, Richard Hofstadter. Hofstadter's argument touched off a firestorm of debate, which continues into the present. With his emergence of the U.S. academy of social history in the 1960s, which sought to recover and celebrate the contributions of non-elite members of American society, Hofstadter was attacked as an elitist and several new histories of the "People's Party" were written that sought to vindicate it from Hofstadter's allegedly baseless claims.[6]

Now, in terms of my own research, because I am familiar with such historical transformations of populism in the European context, I am more willing to entertain Hofstadter's argument. As Charles Postel demonstrated convincingly in his 2007 study, The Populist Vision, there were many genuinely progressive aspects of the late nineteenth-century populist movement in the U.S.; nonetheless, if one looks more closely, it's also not difficult to find many examples of the right-wing populist "herrenvolk republicanism" ideology that Roediger discusses.[7] Postel does not conceal the racist sentiments that surfaced among many members of the populist movement. He and many other scholars have also documented the centrality of anti-finance ideology to the populist movement. He is not particularly troubled by such sentiments, but I do see it as fitting in very well with the larger patterns of right-wing populist ideology in Europe, and with producerist populism, in particular.

How would you compare European right-wing populist movements and U.S. right-wing populist movements such as the Tea Party and President Trump's campaign?

Picking up on my comments in the last section and leaping forward to the present, I would mention only one obvious similarity between European right-wing populist movements and their counterparts in the U.S., namely, the fact that both rely on the personalization of politics I discussed above, and particularly on the demonization of foreigners in general, and Muslims in particular. In a country like France, the right-wing populist party of Marine Le Pen, the Front National, does also draw upon producerist populist ideology. They portray foreigners and Muslims and "freeloading" on the generous French welfare state. In such circles one often hears stories about Muslim women who have multiple children, who make no contribution to French society, but who also expect support from the welfare state. The parallel with the older U.S. ideology of the "welfare queen" is too obvious to need mentioning. But in their recent study of the Tea Party, the Harvard sociologists Theda Skocpol and Vanessa Williamson argue that producerist populism is perhaps the central tenet of Tea Party ideology – even stronger than their anti-government animus, which is usually seen as their core belief.[8] They illustrate this point by showing how most grass-roots members of the Tea Party balked at the attempts of libertarian politicians and think tanks – such as Paul Ryan and the Cato Institute – to convince the Tea Party to support their efforts to dismantle Social Security. So, even though Social Security is a government program, the vast majority of rank and file Tea Party members want to preserve it. They see

> *...one defining characteristic of populism is its ability to mobilize apathetic voters or voters who have a generalized dislike of politics.*

themselves as having worked hard to contribute to it, and they also want to benefit from it. So here we also see a parallel with the situation in France mentioned above. The common theme is that the benefits of the welfare state should be reserved for the deserving, the "virtuous people" and not the "immoral parasites." For the Tea Party, those parasites are "illegal immigrants" who are seen as taking advantage of American institutions – by sending their kids to public schools, receiving government subsidized health care, etc. – without paying any taxes.

Donald Trump's reliance upon such producerist populist ideology is even more obvious than the Tea Party. First, everyone is familiar with his heavy reliance upon xenophobia. But Trump's reliance upon economic populism was much more pronounced than the Tea Party, which – despite the example discussed above – remained basically libertarian in its ideology. Trump's extremely effective campaign strategy was to focus on the nostalgia of the white working class in the upper Midwest for the "good ol' days," when factory jobs were still plentiful and well paid. It seems clear to me that this was how Trump set himself apart from the other candidates in the Republican Primary, namely, by breaking with the laissez-faire economic doctrines that have been an unquestionable article of faith for the Republican Party for as long as anyone can remember. Recent studies of the election have confirmed that it was the white-working class voters who switched from Obama in 2012 to Trump in 2016 and won the election for him.[9] Trump's economic populism was all about restoring the dignity and quality of life of the "virtuous producers" in the "heartland" and punishing the immoral foreigners, both inside – illegal immigrants – and outside – the Chinese, Mexican and even Europe governments, who have been "freeloading" on American largesse – who are responsible for our national decline.

What have been the primary drivers for the success of the Trump campaign, and to a lesser extent, the Sanders campaign?

In addition to what I said above, I would also like to mention Trump's willingness to make use of the anti-finance aspects of right-wing populist ideology. During the Republican primary debates he often criticized his chief rival, Ted Cruz, of taking money from Goldman Sachs. During the presidential campaign he, of course, laid the same accusation at the feet of Hillary Clinton. Now that he's in power and several of his top appointments were themselves long-time employees of Goldman Sachs and other Wall Street banks, the sheer mendacity of Trump's right-wing populist rhetoric is clear for all to see. This, I would argue, is one of the most important differences between right- and left-wing populism. Bernie Sanders also criticized Hillary Clinton ad nauseum for her close ties to Wall Street But if Sanders had been elected, we would justifiably have expected him to not only maintain, but to increase the regulation of Wall Street put in place by the Obama administration after the Great Recession of 2008. Left-wing populists also make use of the "virtuous producers" and "immoral parasites" ideology, but they tend to focus their ire "upwards" at the "wicked bankers," "Wall

Street" etc. But they also – and here Sanders is a good example – come up with concrete and detailed policy plans, to put their ideas into action. Right-wing populism, on the other hand, is always vague about policy recommendations. The focus – and here Trump is a great example – is much more on the prowess of the populist leader, who portrays himself as an outsider, but one who can "clean house" and "get things done." As Trump stated repeatedly at his mass rallies, "I alone can bring about change."[10] The flurry of executive orders during Trump's first week in office clearly sought to reinforce this image of Trump as a "man of action" and not words. Here, too, we see clear parallels with classical fascist rhetoric that democracy is mired in interminable and ineffectual discussion. Trump gave the Tea Party movement what it was lacking; in fact, what it claimed it did not want: an authoritarian leader. But studies have shown that the vast majority of former Tea Party members voted for Trump. I would argue that Trump's producerist populist rhetoric played an important role in garnering this support.

Regarding Sanders, what's important, I think, is to realize just how surprising his success was. I remember many, many conversations with academic colleagues who gave his campaign absolutely no chance of going anywhere. David Brooks' smug response to Sanders' entering the race – "there aren't enough sociology professors in the country for Bernie to win" – is a good example of just how wrong educated elites were about Sanders. The key to Sanders' success, in my opinion, was that he offered a mirror-image of the Trump campaign. Like Trump, Sanders sought mainly to win white-working class votes. Whereas Trump was trying to win them from the Democrats, Sanders was trying to win them back from the Republicans – for whom many of them had been voting since Reagan in 1980. Sanders' economic populism was remarkably successful, but his decision to cater primarily to whites also proved to be his downfall. He was never able to overcome the lead that Southern African-American voters gave to Hillary Clinton in the first stage of the primary. Here again, perhaps, we see African-Americans all too justified suspicion of populist rhetoric. Sanders tried hard to reach out to African-Americans as the campaign went on, and many began to support him. But it was too little too late. In any case, Sanders spoke clearly to the very real issues of rising inequality in the United States, and the massive transfer of wealth upwards that has occurred in the U.S. under the neo-liberal policies of both Republican and Democratic administrations since 1980.[11] The much discussed "populist mood" among the American electorate during the past election is nothing more than a product of the disgust with such rising inequality. Sanders and Trump succeeded because they both spoke openly about it – the former honestly, the latter mendaciously. But even Trump's mendacious gestures to the suffering of the virtuous producers in the "heartland" sounded much better than Hillary Clinton's half-hearted efforts to demonstrate that she actually cared about the brutal inequality that exists in the U.S. It seems that Hillary Clinton, her advisers and other sheltered members of what the populist right loves to call "the liberal elite" are the only ones who haven't realized that neo-liberalism has lost its ideological legitimacy. Both Sanders and Trump demonstrated just how widespread the desire has become to come up with an alternative to neo-liberalism and to rein in the power of entrenched elites in our society.

How effective have populists movement in the U.S. (right and left) been in capturing votes from undecided voters?

Here I will only mention briefly that one defining characteristic of populism is its ability to mobilize apathetic voters or voters who have a generalized dislike of politics. Here's where the strong anti-establishment rhetoric of populism proves very effective. Donald Trump portrayed himself – in typical right-wing populist fashion – as a political outsider who would "clean house" in Washington D.C. and would "get things done." If one studies the history and content of right-wing populist ideology in the U.S. – as Leo Lowenthal and Norbert Guterman did in the 1940s – one frequently encounters the theme of "running the country like a business."[12] Lowenthal's colleague at the Frankfurt-based Institute for Social Research, Theodor Adorno, analyzed this desire on the part of right-wing populist agitators and their supporters to replace the democratic political process with the much more authoritarian business model, with president acting as the C.E.O., in terms of what he called "pseudo-conservatism."[13] Adorno distinguished "pseudo-" from "genuine" conservatives in terms of the latent authoritarian dispositions that exist among the former. As Adorno put it, "The pseudoconservative is a man who, in the name of upholding traditional American values and institutions and defending them against more or less fictitious dangers, consciously or unconsciously aims at their abolition."[14]

The genuine conservative, on the other hand, is presumably a person who would never be willing to sacrifice basic constitutional rights, such as the freedom of speech (including the freedom to protest in the streets) and freedom of religion (for all religious groups, including Muslims). I think that Adorno's distinction between pseudo- and genuine conservatives can still shed very much light on recent developments within the Republican Party; Trump's victory certainly represents a triumph of the authoritarian pseudo-conservatives over the entrenched traditional conservatives. But the idea of "running the country like a business" comes straight out of the right-wing populist playbook and appeals to pseudo-conservatives' desire for more authority and less of the messiness, tolerance and compromises that come with genuine democracy. In this sense, I think Trump was successful in mobilizing apathetic and disaffected voters who may otherwise not have voted at all. Studies have shown that even taking a serious interest in politics is considered "elitist" by many Americans. Right-wing populists' harsh words against "politicians" and "Washington" are well received among people like this.

How large a role do you think use of digital media - not only from the campaigns but from supporters - had on the Trump and Sanders campaigns?

Not being an expert in this area, I would only like to mention Trump's use of Twitter, insofar as it resonates with some of my research on the history of right-wing populism. As Freud pointed out in his Group Psychology and Analysis of the Ego, crowd psychology, or what he described as collective narcissism, is predicated upon the psychological mechanism of identification. Powerful groups can be formed when followers subordinate their own ego to the collective ego of the group, which is embodied in the leader of the group. This technique can be observed by watching any National Socialist mass rally at which Hitler spoke. Over many years, Hitler perfected the technique of speaking at mass rallies in a way which would encourage this type of psychological identification among his followers. It was not a coincidence that one of the few mass produced consumer goods that the Nazis made cheaply available to the German people was the so-called Volksempfanger, or "people's radio." They wanted every German family to have a radio in their house, so they could listen directly to Hitler's speeches. Television had not, of course, been invented yet. But here we can see one example of the Nazis' remarkable skill in utilizing the "new media" of their time to consolidate their power. Film was another example, but I won't go into that here. In any case, it's hard for me not to see a striking similarity between Trump's reliance upon Twitter and the Nazis' use of radio to encourage psychological identification with the leader in the manner described above. To be clear, I'm not saying here that Trump is a fascist or that he was in any way as terrible or threatening as Hitler. I don't think he is. But I do see fascism as an extreme and National Socialism as perhaps the most extreme form of right-wing populism. Right-wing populist parties that exist today continue to draw upon many of the same tactical and ideological devices of other right-wing populist movements in the past. This is also why it's important to study the history of right-wing populism. "Fascism was not a coincidence," as Adorno once put it. There are powerful social and social-psychological forces at work in our societies which give rise to right-wing populism. So we need to understand not only right-wing populism itself, but also these deeper social and social-psychological forces that give rise to it. In any case, Trump's use of Twitter seems to me like a more advanced technological means of establishing a "direct link" between the leader and his followers.

What's crucial for right-wing populism, in particular, is that the leader establishes himself as the direct embodiment of "the people" who represents the "general will" and has the power to define and punish "enemies of the people." Any intermediary bodies between the leader and "the people" are supposedly eliminated. Trump does try to use Twitter in this way, to lash out at anyone who criticizes him and to attempt to portray them as "enemies of the people." How effective he is in this regard is open to question. But those who identify with him and see him as embodying their own will, certainly appreciate this perceived "direct link" with the leader. Regarding left-wing populism, it doesn't need to rely on this type of mechanism of identification as much as right-wing populism, insofar as it puts more emphasis on concrete policy proposals and less emphasis on eliminating "enemies of the people." But it's not difficult to give examples of this type of leader-follower identification among left-wing populists. Hugo Chavez comes immediately to mind. The big question for left-wing populist movements is whether or not they succeed in putting progressive institutions in place, which can survive the death of a charismatic leader. When left-wing populist movements become too focused on a charismatic leader, it's a threat to their ability to create lasting change.

What are critical factors would you identify for the successful future of the right-wing populist movement in the U.S.? The left-wing?

I think that as long as economic inequality and uncertainty remain as high as they are in the U.S. (and Europe) right now, populist movements will continue to flourish. In Europe, where there is a much longer and deeper tradition of socialism than in the U.S., my hope is that new democratic socialist movements and parties will emerge that break with the deeply problematic legacy of "new" Labor in Britain and – to a lesser extent – "new" social democratic parties on the Continent, which adopted many aspects of the new neo-liberal economic orthodoxy in the 1990s. When asked what she saw as her greatest achievement, Margaret Thatcher famously responded "New Labor". We see the same thing happen in the U.S. under Bill Clinton. In terms of promoting free trade, deregulation, neo-liberal globalization, and slashing the welfare state, Clinton was every bit, if not more zealous than his Republican predecessors. Syriza in Greece seemed, for a moment, to represent the possibility of the re-emergence of a viable democratic socialist alternative in European politics. But it ran aground on the fundamentally neo-liberal principles of the

European Economic Union, which were staunchly defended by Germany.

In any case, I see this rather dramatic movement of Social Democratic, Labor and Democratic parties in Europe and the U.S. toward the neo-liberal center in the 1990s (and earlier) as one of the most important reasons for the rise of right-wing populism in Europe and the U.S. In the absence of a vigorous left-wing critique of capitalism and neo-liberal globalization, those who suffer most from pro-market and austerity policies will be easy prey for right-wing populist critics of globalization and the European Union. In the U.S., where socialist traditions are much weaker, I don't see any realistic alternative to left-wing populism of the sort represented by Bernie Sanders. Looking back on his campaign, he did many things right. He was much more successful than anyone expected him to be. But, as already mentioned, perhaps the single greatest cause of his failure to win the nomination against Hillary Clinton was his failure to win the support of that most solid block of Democratic voters: African-Americans. It seems clear that the success of a left-wing populist movement in the U.S. will need to create a new alliance between the so-called "white" working class, and the rest of the working class, and progressive members of the middle class, both white and people of color. But the very fact that the "white" working class consciously or unconsciously still views itself as the "virtuous producers" and everyone else as "freeloading" off of their hard work, presents a massive barrier to such a progressive coalition. If members of the white working and middle class could see people of color as their allies, and wealthy elites like Donald Trump as their real enemies, then the possibility of a left-wing populist coalition would emerge. Don't hold your breath.

John D. Abromeit is Associate Professor of History and Social Studies Education at The State University of New York (SUNY), Buffalo State. His books include *Transformations of Populism in Europe and the Americas: History and Recent Tendencies*, co-edited with Bridget Chesterton, *Max Horkheimer and the Foundations of the Frankfurt School. Herbert Marcuse: Heideggerian Marxism*, co-edited with Richard Wolin, and *Herbert Marcuse: A Critical Reader*, co-edited with W. Mark Cobb.

Trump's Tea Party

Professor Kristin Haltinner
University of Idaho

Social media and increased access to internet-based forms of communication have revolutionized the spread of right-wing populist ideas. Propaganda, op-eds, news stories, and other types of information spread quickly through online forums, enabling discourse to evolve swiftly and citizen organizing to coalesce with great expediency. One example of the power that the digital age has given to right-wing populist movements can be seen in the Tea Party and its creation of a political opportunity for the election of Donald Trump. This piece argues that the Tea Party, and its novel employment of social media, created a discursive space for Trump's rhetoric (specifically a rejection of political correctness, intellectualism, and political insiders) and policy initiatives that ultimately contributed to his election.

The Rise of the Tea Party

The Tea Party was launched in response to the 2009 "rant" of CNBC Reporter Rick Santelli. In this speech, Santelli called for a "Chicago Tea Party" primarily focused on resisting the housing bailout proposed by Obama. The Tea Party's main goals include promoting government fiscal responsibility, limiting government control, and bolstering free market capitalism.

Concurrent with the rise of the Tea Party was an increase in broad access to various forms of social media, including Facebook and Twitter. Indeed, between 2008 and 2012 the number of people using some type of social media increased from around 20% to around 60% (Pew Research 2017). In stride, Tea Party activists tapped into these forums in unprecedented ways for social movement organizations. Don Tapscott, co-author of *Macrowikinomics*, in an interview with Derek Thompson of *The Atlantic*, argues that the Tea Party masterfully employed the Internet to build a "massive political movement." While previous media operated on a centralized model reflecting the values of media owners, Thompson argues that the "new media" is less beholden to corporate control and free to engage with and distribute (as news sites are beginning to charge for content). This allowed the Tea Party to freely share information and propaganda quickly across the nation and connect local organizations to national discussions about right-wing politics (Hiar 2010).

The use of social media also allowed Tea Party activists to control political discourse, rather than relying on corporate news sources to share stories they deemed relevant. Raynauld (2013) examines the Tea Party's use of Twitter, specifically, and finds that the Tea Party engaged with social media in novel ways, a distinct departure from social and political movements operating earlier. The Tea Party's use of Twitter for example, empowered a wide breadth of activists to participate in the movement and spread the party's ideology (whereas previous movements relied heavily on their leadership for information sharing). This further led to the organization having greater control over the narrative about current events. Thus, activists promoted and discussed a large array of political issues, regardless of whether or not major news outlets were interested in the topics early on, ultimately forcing news outlets to cover these issues. Beyond shifting political discourse, the Tea Party used social media sites to conduct political action. It mobilized online activism as the organization encouraged activists to take on efforts such as giving bad ratings to progressive books or promoting right-wing digital content through cunningly abusing Google's algorithms (Hiar 2010).

Through their use of online media, the Tea Party had a profound impact on culture. The process of influencing discourse can have particular influence on broader society as it is the spread of this knowledge that truly indicates the power of right wing movements to influence society through changing culture (Rochon 1998), shaping public policy (Burnstein 1999), and reconstructing social categories while policing their content (Berlet 2000). A powerful measure of movement success is the production of new ways of thinking and behaving in broader society (McAdam 1994, Rochon 1998).

Political Opportunity for Trump

Theories within the field of political sociology argue that the formation of social movements – in this case a political movement regarding the election of Donald Trump – happens when a) a group of people holds a shared grievance against a particular system they find unjust (Meyer 2004); b) the group has the material means to organize (Tarrow 1998); and c) a political opportunity – or some sort of amenable shift within the political fabric of society (Tarrow 1998; McAdam 1982). With respect to the election of Donald Trump, a variety of events and political shifts opened the political arena for the group's emergence. One significant contribution was the Tea Party and its use of the Internet to both shape the actions of the Republican Party and change cultural discourse more broadly.

The Tea Party was a major drive in shifting Republican politics from 2010-2016. While some argue that the Tea Party has become the Republican base (Arrillaga 2012), at the very least it has pulled the party to the right (Bischoff and Mallow 2012). By the fall of 2011, 41 percent of voting Americans who participated in exit polls said that they supported the Tea Party. In April of 2012, the same percentage of people reported support for the organization. Regarding elections in particular, the Tea Party elected 32 percent of the 138 candidates it backed in 2010; 40 percent of the ten candidates they endorsed in 2012, most of whom continued to hold office in 2016 (Zernike 2010). The Tea Party has also continued to receive validation from media outlets as exemplified in the airtime given to them, in addition to the Republican Party, following the 2013, 2014, and 2015 State of the Union Addresses. Thus, it is clear that the Tea Party continues to be placed in a position to affect national and local politics.

What may be further evidence of this is the perceived influence the Tea Party had on Republican politics. For example, the Tea Party is credited with effecting Romney's campaign, leading him to lobby for "some tea party-friendly positions" and pepper his speeches "with lines that play to the tea party crowd" (Arrillaga 2012). The Tea Party is recognized for the success of Governor Scott Walker of Wisconsin, and conservative legislatures elsewhere, in curbing the strength of unions in their respective states (Greenhouse 2011). While early polls showed that Tea Party members supported a number of different Republican Candidates for President in 2016, including Ron Paul; Ted Cruz; and Donald

Tea Party activists created space for and continue to celebrate Trump's rejection of political correctness.

Trump, the Tea Party Super PAC ultimate threw its support fully behind Trump.

In the seven years of its operation prior to the election of Donald Trump, the Tea Party drove changes in public discourse that created a political opportunity for Trump's election. Specifically, they shifted cultural narratives to a) reject previously held values such as political correctness and intellectualism, b) reject political insiders and traditional politicians, and c) support policy initiatives that mirrored those rejections.

Tea Party activists created space for and continue to celebrate Trump's rejection of political correctness. During their tenure as a powerful social movement organization, they rallied loudly on social media against linguistic consideration for marginalized groups: from rejecting political correctness outright (even proposing legislation to ban political correctness), to criticizing the use of "trigger warnings" when discussing potentially traumatic issues. This created an opportunity for Donald Trump to embrace extreme rhetoric and be met with the support of the Tea Party. Trump has rallied against the "War on Christmas" exemplified by people saying "happy holidays" instead of "Merry Christmas". He blatantly expresses his refusal to be political correct and regularly makes overtly offensive statements about Mexican people ("rapists"), women ("fat pigs", "dogs", "slobs", "disgusting animals"), and other marginalized populations.

While anti-intellectualism is not a new discourse within U.S. politics or the Republican Party (Hofstadter 1963; Boot 2016), the Tea Party reenergized a right-wing populist discussion regarding perceived left-wing elitists. Through the online spread of memes and ideologically slanted news stories, they routinely celebrated politicians who rejected science, such as Michelle Bachman and Sarah Palin, and scorned those who spoke eloquently, as "out of touch" or snobbish. In the end, this narrative created space for the election of a man who lacks extensive education, who openly rejects intellectualism, and whose public speaking engagements are often befuddling and unclear in their rhetoric, repetition, and inaccuracy. For instance, since becoming president, Trump did not know how many articles there are in the Constitution, regularly touts conspiracy theories, and celebrates that he makes decisions "with very little knowledge" about a subject in exchange for efficiency.

Above all, the Tea Party created an opening for Trump in their rejection of political insiders. The Tea Party narrative underscored politics-as-usual, particularly democratic policies had tainted by all the "career politicians", who they see as inept, corrupt, and easily bought by lobbyists. Trump was able to embrace this narrative, identifying as a political outsider, and find support among Tea Party activists.
In addition to creating political space for the rhetoric employed by Trump, the Tea Party also paved the way for some of his more extreme policy initiatives. For example, Trump's vow to build a wall on the U.S.-Mexico border, his promises to empower Christian values, his battle against the EPA, and, most importantly, his promise to repeal the Affordable Care Act, all mirror Tea Party positions. Further, the

extreme nature of his positions reflect ideologies touted by the Tea Party over the preceding years, thus making them more palatable to many Americans.

Engagement with social media is a powerful way to circulate knowledge and power in society. Unlike social movement organizations before them, the Tea Party engaged extensively with sites such as Facebook and Twitter to spread their ideology. This enabled the organization to share information and propaganda quickly and widely, ultimately popularizing a rejection of political correctness, intellectualism, and political insiders. Populist engagement with these narratives ultimately created a political opportunity for the election of Donald Trump.

Kristin Haltinner is an assistant professor of Sociology and Director of the Certificate in Diversity and Stratification at the University of Idaho. Her research is on right-wing ideology and social movement organizations; racial formation and discourse; and social inequality. Her recent projects focus on the TEA Party Patriots and the Minutemen Civil Defense Corps.

Populism Down Under: the rise, fall, and resurgence of Pauline Hanson and the One Nation Party

Professor Zareh Ghazarian
Monash University

I In July 2016, Pauline Hanson made a spectacular political comeback. After an 18 year absence, the charismatic leader of Australia's preeminent populist party returned to the national parliament. The 2016 result was even more remarkable as Hanson led her One Nation Party to its best ever election result by winning four seats in the Australian Senate. The re-emergence of One Nation has been seen to be part of a developing global movement of disillusioned citizens in liberal democracies mobilizing around populist political leaders. Such sentiment is strengthened especially in light of the recent decision of the United Kingdom to leave the European Union as well as the rise of Donald Trump as President of the United States. But is Hanson's resurgence in Australian politics part of a global movement or is it due to the domestic political debate and quirks of the electoral system?

To find out, I consider the reappearance of Hanson and her brand of populist politics in Australia. To be able to make sense of the One Nation phenomenon, I firstly consider the distinctive parliamentary and electoral system of the Australian system. It is also crucial to chart the evolution of minor parties from the political right in Australia before analyzing the electoral performance of One Nation in 2016. I conclude by putting the return of Pauline Hanson into perspective and show that, while One Nation may be back in the national parliament, its future in Australian politics is less than certain.

The Australian system of politics and government

As Australia follows the Westminster system, government is formed by the party (or coalition of parties) that wins a majority of seats in the House of Representatives. The chamber, also known as the lower house, has been dominated by the Labor Party and non-Labor parties since federation in 1901. In the post-war period, the largest non-Labor party has been the Liberal Party which has been in a formal coalition with the Nationals Party. The Liberal Party was created in 1944 while the Nationals was created with the specific aim of advancing the interests of rural and regional constituencies in 1920. Together, they have been the major right of center force in Australian politics.

The Australian parliamentary system also has a powerful Senate, known as the upper house, modeled on the American system and designed to be the "state's house" in which the interests of individual states would be pursued. This concept is reinforced by the fact that all states, irrespective of their population, are represented by the same number of senators.[1] The Senate has the same powers as the House of Representatives, except that it cannot initiate or amend supply and taxation bills.

Aside from its structural importance, the Senate is the chamber in which minor parties have won parliamentary representation, sometimes wielding the balance of power and exerting significant influence over the policies of governments. Furthermore, the term for the House of Representatives is three years while senators are elected for six year terms. This means that minor parties may be present in the Australian parliamentary system for a significant period of time. All senators, however, are up for election when a double dissolution election is called, as was the case in 2016. A double dissolution election occurs when both the Senate and the House of Representatives are dissolved and every seat in both chambers is contested. Such an election may be called by the prime minister when there is a deadlock between the two houses of parliament.[2]

The Australian electoral system

The major parties have dominated election contests in Australia. Just three parties other than the Labor and Coalition parties have won seats in the House of Representatives at general elections in the post-war period.[3] A significant factor contributing to this situation is the electoral system. The House of Representatives uses single member districts and the Alternative Vote. In the Senate, however, a single transferable vote method of proportional representation has been used since 1949. As Duverger (1954:217) reminds us, majoritarian systems like that used in lower house elections lead to a chamber dominated by two political forces. Conversely, a system of proportional representation, as used in Senate contests, leads to a chamber filled with many parties (Duverger 1954:239). Indeed, non-major parties have been able to win seats in the Senate far more often than in the lower house since the introduction of proportional representation. This has allowed them to exert significant influence over the policies of government.

In 1983, the incoming Labor Government led by Bob Hawke implemented a series of reforms to the Senate voting system. These reforms included expanding the number of senators per state from 10 to 12.[4] This reduced the size of the electoral task confronting minor parties as it reduced the percentage of the vote needed to achieve a quota to win a seat in the chamber. Rather than having to win 16.6 per cent of the statewide vote at a general election, candidates could now win a seat with just 14.4 per cent. This rate is halved at double dissolution elections, making it even easier for candidates to win Senate representation. Public funding for elections was also introduced and meant that candidates would be entitled to receiving a set payment if they won at least four per cent of the primary vote.

Another crucial reform was the introduction of the group ticket vote (GTV), which the government described as a much simpler method of voting for the Senate. By simply indicating their first preferences, voters would have their preferences distributed by the electoral commission in accordance with the voting ticket lodged by their preferred party (see Sawer 2004). The rate of GTV use is especially high (between 98 and 99 per cent) for electors voting for the major parties. The introduction of the GTV was also boon for new parties as they could engage in making preference deals with other parties in order to enhance their own prospects of winning Senate representation.

Election results show that just three new parties won seats in the Senate between 1949 and 1983. In contrast, 12 new parties were elected to the Senate since changes to the voting system were first used in 1984. In 2016, the Coalition government made further changes to the Senate voting system. A key reform was the introduction of optional preferential voting. While it is expected that these reforms will limit the capacity for candidates to make preference deals, the reforms have yet to be used at a general election.[5]

Right-populist parties in Australia

A number of minor parties won Senate representation between 1949 and 1996, but none represented the right-populist type. While it is difficult to provide a concise and universally accepted definition of populist politics, much research has identified core characteristics of right-populist parties. As Betz (1998:4) summarized, such parties espoused a "pronounced faith in the common sense of the ordinary people", that "simple solutions exist for the most complex problems of the modern world", and that "the common people, despite possessing moral superiority and innate wisdom, have been denied the opportunity to make themselves heard." Additionally, Hainsworth (2000:11; 13) identified opposition to "immigrants, asylum seekers and refugees" as "important vote-winners" for such parties. Moreover, it is the right-wing populist candidates' responses to "fix" these areas which adds another dimension to their presence in the political system. As Hainsworth (2000:14) argued, these candidates believed that the "mainstream and establishment forces" had "failed" and offered "new" and seemingly "straightforward alternative politics." As Betz (1993: 413-4) summarized, right wing populist candidates often appealed 'to those disenchanted with their individual life chances and the political system'.

In 1998, One Nation became the first minor party which resembled the right-populist type elected to the Australian Senate. The One Nation Party was created by Pauline Hanson who had built a high public profile while serving as an independent MP from Queensland in the federal parliament since 1996. Hanson had previously been a member of the Liberal Party but was expelled when she made controversial comments about race and immigration prior to winning a seat in parliament. Hanson argued that "reverse racism" was occurring and felt that indigenous Australians were being advantaged at the expense of "white" Australians. Hanson also presented herself not as a "polished politician", but as a "woman who…had her fair share of life's knocks" (Hanson 1996: 3860). Hanson quickly established herself as an anti-establishment politician. She had operated a small takeaway shop prior to being elected to parliament and railed against the established parties' platforms of multiculturalism and cosmopolitanism. Hanson's popularity grew especially as she also attacked the major parties' acceptance and promotion of economic rationalism which she argued were negatively impacting "ordinary Australians." Hanson's attacks on the economic status quo, and her stated desire to represent "average" citizens, reflected the right-populist approach and resonated with sections of the electorate.

In particular, Hanson's emergence was a threat more for the Coalition than Labor as One Nation was gaining its strongest electoral support in rural and regional electorates which were previously Nationals Party heartland. While Hanson continued to campaign on race and immigration matters, it was ultimately her outright rejection of economic liberalization that resonated most with these electorates. This was particularly potent at a time in Australian politics when state and national governments sought to privatize formerly state-provided services while advancing the benefits of globalization. This approach contributed to a growing sense in these rural and regional electorates that successive governments were no longer advancing their interests. The Nationals suffered the most electoral damage from the rise of Hanson as she was effective in arguing that they had abandoned advancing the interests of rural and regional communities and were now strong supporters of the Liberal Party's economic liberalization policies. Indeed, Hanson's protectionist approach appealed to many voters in these electorates who were experiencing the uncertainties of a changing labor market (see Mughan, Bean and McAllister 2003).

One Nation performed strongly in the 1998 national election, but it could only win one Senate seat in Queensland as the major parties used the electoral system to deprive the party of preferences. While the party won seats at subsequent state elections, the party floundered at the federal level. At the next national election in 2001, Pauline Hanson lost her lower house seat and, in 2003, was sentenced to three years in prison for fraudulently registering the One Nation Party (see Crime and Misconduct Commission 2004). She successfully appealed her conviction and was released two and a half months later. Without Hanson, however, One Nation struggled for media attention and relevance in the political debate.

Hanson, on the other hand, maintained a remarkably high public profile following her initial term in parliament. She left One Nation and contested subsequent federal and state elections as an independent. Hanson also appeared regularly in the media as a commentator and published her biography which garnered much attention. She was also regularly on television and appeared on entertainment programs such as *Dancing with the Stars* which led to some describing her as a "rolled gold celebrity" (Kingston 2007). Despite this high public profile, Hanson remained unable to win parliamentary representation and it appeared that One Nation was a spent political force.

After One Nation: Parties from the right in the Senate from 2004 to 2013

Following the demise of One Nation, new minor parties from the right won Senate representation. In 2004, the Family First Party won its first seat after arranging a series of beneficial preference deals with the major parties. The party sought to advance a conservative range of policies on social and moral issues and opposed same-sex marriage, euthanasia, and the availability of pornography. Family First forged a role in Australian politics as an anti-Greens party, especially as it opposed the socially progressive policies of the Greens. It won another seat at the 2013 election and held that seat at the 2016 double dissolution election.

The Democratic Labor Party (DLP) also won Senate representation following One Nation's disintegration. While the DLP was initially created as a result of a split in the Labor party in the 1950s, the 'new' DLP elected to the Senate in 2010 was qualitatively different to its progenitor. Rather than be concerned about opposing Labor, the modern DLP, like the Family First Party, sought to advance a conservative moral agenda that opposed the progressive policies of the Greens. Unlike Family First, however, the party could not consolidate its position in the Senate in subsequent elections, primarily due to its inability to manufacture preference deals with the major parties. Neither party, however, could be seen to be right-populist parties.

The seeds of current populism from the right in Australia were sown at the 2010 national election.

The 2013 election: Reigniting the Hanson flame

The seeds of current populism from the right in Australia were sown at the 2010 national election. Just before the election the Labor Government replaced Prime Minister Kevin Rudd, who led the party to victory in 2007, with his deputy Julia Gillard. As Australia's first female prime minister, Gillard led a divided Labor Party to a relatively poor election outcome in which neither Labor nor the Coalition won a majority in the lower house. The result was that both parties had to negotiate with the Greens MP, as well as independent MPs, in order to form a majority. After two weeks of negotiations, Gillard was ultimately successful in garnering the support of these MPs and formed minority government.

The policies the Gillard Government pursued, however, mobilized right-populist parties in Australia (see Economou 2015). As part of the agreement between Labor and the Greens and independent MPs, the Gillard government redoubled its efforts to address climate change. It implemented a mining tax and advanced conservation policies, such as establishing a major marine national park, which concerned many in regional electorates because they could undermine employment prospects (see Economou 2015:347). The government also sought to broaden protections for national parks which would constrain recreational activities. This mobilized many, especially those who took part in shooting and fishing, against the government. As one commentator noted, the Gillard Government had 'made an extensive array of enemies' with its socially progressive policy program (Economou 2015:347).

The most controversial policy, however, was the Gillard government's implementation of a carbon pricing scheme, which quickly became known as the "carbon tax." This was problematic as Gillard had promised that such a tax would not be implemented by her government during the election campaign (Butcher 2014). This mobilized significant opposition across the electorate. Moreover, it appeared that the government was beholden to the Greens and favored an agenda that would support progressive, cosmopolitan ideals rather than advance the interests of "ordinary Australians." Indeed, the carbon tax became a political problem for Gillard. Her government's popularity fell dramatically and precipitated her removal as Labor leader. She was replaced by former prime minister Kevin Rudd who led the Labor Party to a heavy election loss at the national election held in 2013.

The electoral system meant that the Coalition benefited from the anti-Labor swing in the lower house. The electoral system in the Senate, however, provided non-major parties with the opportunity to exert influence on the political debate (see Economou 2015:350). In fact, a record 54 parties had registered to contest the election. This compared to just 25 in 2010 (see Green 2013). As Table one shows, the rising number of parties contesting the election was due to the increased numbers of non-major parties from the right.

Table 1: Number of Non-Major Parties from the Left and Right Contesting Australian Federal Elections, 1985-2016

Election year	Parties from the left	Parties from the right	Centrist parties
1984	3	4	2
1987	5	10	1
1990	9	13	2
1993	5	13	2
1996	4	13	1
1998	3	17	1
2001	8	19	1
2004	6	17	1
2007	4	16	1
2010	7	13	1
2013	10	34	2
2016	11	33	6

Source: Economou, N. 2016. 'Electoral reform and party system volatility: The consequences of the group vote ticket on Australian Senate elections'. Australasian Parliamentary Review. 31, 1:117-130.

Table one shows the number of non-major parties peaked at 19 between 1984 and 2010. Indeed, the number of non-major parties from the right was actually falling between 2001 and 2010. In 2013, however, the number of non-major parties from the right shot up to a record 34. The bulk of these parties had mobilized to oppose Labor's "carbon tax" and environmental policies (see Economou 2015:351).

Despite signs of a growing rapprochement between Hanson and One Nation, the party did not perform particularly strongly at the 2013 poll. Instead, a number of other minor parties from the right won Senate representation at One Nation's expense. The most prominent was the Palmer United Party which was created by wealthy business man Clive Palmer just before the election. The party won three Senate seats and a Queensland lower house seat which was a remarkable achievement for a nascent party. The Palmer United Party railed against Labor's policies and criticized the major parties for ignoring the policy demands of "ordinary Australians." Led by the charismatic Clive Palmer, the party promised to advance the interests of "ordinary voters" with the view to enact protectionist policies to keep manufacturing jobs and safeguard the interests of primary producers in rural and regional electorates. The party, however, soon encountered internal instability. Two of its three senators resigned from the party and continued their parliamentary careers as independents and, by the time of the 2016 election, the party had disintegrated.

Two additional parties from the right were elected to the Senate for the first time in 2013. The Liberal Democrats and the Australian Motoring Enthusiasts Party won a seat each. The former based on libertarian ideals and opposing the "nanny state", while the latter was concerned with safeguarding the "Australian way of life" from the policies of "irresponsible" minorities (Liberal Democrats 2016;

AMEP 2013). The success of minor parties from the right at the 2013 election was encouraging for Hanson. While neither party reflected the brand of populism advanced by Hanson, their performance demonstrated that there were segments of the electorate who supported a social and policy agenda that countered the major parties' approaches.

Back in the Senate: Pauline Hanson's One Nation 2.0

Prior to the 2016 election, Hanson formally rejoined One Nation and the party began to attract significant media attention once more. Like 1998, race and immigration were central to the party's platform as was concern about the "Australian way of life" being eroded by immigration and globalization. In 2016, however, the party broadened its anti-immigration stance to specifically focus on Muslim migration. One Nation promised to hold an "inquiry or Royal Commission to determine if Islam is a religion or political ideology" as well as "stop further Muslim Immigration (sic) and the intake of Muslim refugees until we can assure the safety of Australians" (PHON 2016a). The party also sought to "ban the Burqa and Niquab (sic) in public places" as well as install surveillance cameras in Mosques and Islamic schools (PHON 2016a). Furthermore, Hanson expressed concern about the availability of Halal food. As the party stated, by "buying Halal certified products, it means that you are financially supporting the Islamisation of Australia, including Sharia Law, which opposes our Australian Constitution and democracy" (PHON 2016b).

One Nation also redoubled its attacks on the major parties' economic policies. It criticized the approach of Labor and Coalition governments for appearing to be beholden to foreign forces. For example, the party promised to "restore Australia's constitution so that our economy is run for the benefit of Australians instead of the United Nations and unaccountable foreign bodies that have interfered and have choked our economy since the federal government handed power to the International Monetary Fund in 1944" (PHON 2016c). Moreover, the party promised that it would implement policies, such as cheap energy, in order to 'restore manufacturing, jobs and exports' as well as reduce the cost of living (PHON 2016c).

These policies ensured Hanson received significant media attention during the 2016 campaign that meant the party did not need to invest in traditional or digital campaigning methods. Rather, Hanson used the media to disseminate her messages as well as advance her policy agenda by regularly being invited on current affair programs and through daily coverage of her campaign by media outlets. It was not only the media that was fascinated with Hanson's re-emergence. Both the prime minister and opposition leader also engaged with her views through the media. Prime Minister Turnbull, for example, stated that "Pauline Hanson is, as far as we are concerned, not a welcome presence in the Australian political scene" (see Gothe-Snape 2016). Similarly, the leader of the opposition attacked Hanson for advancing "the politics of fear and hate" and that "Australians didn't like her views then, they won't tolerate them now" (Gothe-Snape 2016). These statements played into the hands of Hanson as she was able to consolidate her position as an anti-establishment figure who was railing against the political elites.

Despite such a high public profile, One Nation won just 1.3 per cent of the national primary vote in the House of Representatives in 2016. This was significantly lower than the result in 1998 when the party won 8.4 per cent of the primary vote in the lower house. Much of this downturn was due to the fact that One Nation only contested 15 seats in 2016 compared to 135 in 1998. A similar fall was apparent in One Nation's Senate performance as the party won just 4.3 per cent of the national primary vote in 2016 compared to 9 per cent in 1998. A significant factor that reduced One Nation's primary vote was the fact that there were almost double the number of minor parties from the right contesting the 2016 election as there were in 1998. While each of these minor parties from the right won a very small percentage of the primary vote (in many cases less than one per cent), the sheer number of such parties chipped votes away from One Nation.

A disaggregation of the Senate electoral performance reveals the support base of One Nation and explains how the party won more seats in 2016 with a drastically lower primary vote than 1998. The party's strongest performance was in Hanson's home state of Queensland where One Nation won 9.2 per cent of the primary vote. As the quota needed to win a seat at the double dissolution election was about 7.7 per cent, it meant that the party actually won 1.2 quota and allowed Hanson to win her seat without the need for preferences while her running mate was also elected on the back of a flow of preferences. The party also won Senate seats in New South Wales and Western Australia with a primary vote of just over 4 per cent which meant the party had to attract a small number of preferences to claim Senate seats which duly occurred.

Putting it into perspective: One Nation and populism in Australia

Analysis of One Nation's performance in its strongest state of Queensland shows that the party achieved its best support in rural and provincial areas which had a relatively high proportion of people with low incomes, unskilled occupations and low education levels (see Nelson 2010). One Nation's performance was weakest in metropolitan electorates where there was a relatively high proportion of people with high incomes, professional occupations, and tertiary qualifications (see Nelson 2010). Indeed, this pattern of support was apparent in Western Australia and New South Wales in which One Nation also won Senate seats.

The pattern of One Nation support also shows that its message resonated outside of the major city centers. Indeed, Hanson's message did not resonate in metropolitan seats in which there are wide ranging opportunities for economic and educational advancement. Rather, support came from rural and regional areas which have fewer opportunities than the "city-based knowledge-worker heartland" (Salt 2017). These districts, however, are where the Nationals Party has traditionally achieved its strongest electoral support. But, after appearing to support the Liberal Party as part of a coalition arrangement on broad economic policy, the Nationals seemingly drove parts of its constituency into the hands of One Nation.

Conclusion: Hanson and the future

It is easy to overstate the re-emergence of One Nation as part of a global anti-establishment phenomenon. A closer examination of the party's performance in 2016, however, casts doubt on such an argument. After all, the party won a significantly lower percentage of the vote in the 2016 election compared to its performance in 1998. Like 1998, the party's support in the latest election came from rural, provincial and regional areas which had communities concerned about the major parties' progressive, globalized policy agenda.

In speculating the future of One Nation, two significant challenges confront the party. First, it has limited electoral support. The fact that the 2016 election was a double dissolution meant it was much easier for One Nation to win Senate seats. It is expected that the next election will be an ordinary election in which only half of the Senate will be up for election which will double the quota needed to win a Senate seat. Second, the changes to the electoral system implemented in 2016 will make it even more difficult for the party to win Senate seats on the back of preference deals. While Pauline Hanson continues to attract much media attention, her party's long term prospects in the Senate may be restricted. The combination of limited electoral support and changes to the electoral system may present insurmountable barriers for One Nation in future contests.

Dr. Zareh Ghazarian is a Lecturer in Politics and International Relations in the School of Social Sciences at Monash University, Victoria, Australia. His most recent book is *The Making of a Party System: Minor Parties in the Australian Senate* (Monash University Press, 2015).

Anti-Chinese Populism in Africa's Digital Age

Professor Steve Hess
University of Bridgeport

Over the last two decades, sub-Saharan Africa (SSA) has witnessed the emergence of China as a critical new outside player on the continent, providing new sources of trade, investment, and assistance. China's bilateral trade has increased rapidly in volume, rising from less than $6 billion USD in 1995 to over $200 billion USD in 2013. Additionally, Beijing has become an important source of foreign direct investment (FDI), its stock of investments exceeding $40 billion USD in recent years. Chinese infrastructure projects, imported manufactured goods, and as many as one million Chinese nationals living and working across Africa have shifted the social and economic landscape.

In the eyes of many African elites, China's appearance has brought a welcomed alternative to traditional partners - in the form of developed Western states and international financial institutions (IFIs) such as the International Monetary Fund (IMF) and World Bank. Whereas economic support and assistance from these sources often come with conditions for economic and good governance political reforms, China's engagement has been characterized with the principle of non-interference and win-win, business-style relationships. As a country that has only overcome many of its own development challenges to emerge as a major world economic power, China provides an inspiring model for African states seeking to uncover a development pathway more in line with local political and economic conditions.

Western critics have often suggested that African support for Chinese engagement is superficial. African elites who seek assistance, investment and trade without the troublesome conditions of Western sources enthusiastically seek deepened partnerships with China. However, average citizens complain of labor and human rights abuses, shoddy and low-quality Chinese goods and infrastructure projects, job loss associated with the influx of cheap Chinese manufactures, and the corrupt bargains struck between local elites and Chinese partners that siphon wealth from natural resources. In spite of such criticisms, public opinion surveys in recent years have found that in general, average Africans hold positive views of China's rising role in their respective countries and the continent as a whole.

Of course, in Africa's digital age, the media landscape has transformed dramatically, transforming the relationship between African states and the mass publics they govern. With rising Internet penetration rates, the rise of social media, and the growing number of local media outlets, African media consumers have a previously unimaginable variety of sources of information and news. These shifts have challenged the ability of incumbent leaders to frame their bilateral relations with China in a positive light and suppress or deflect information that threatens to compromise important deals with Beijing and Chinese firms. In Zambia, for example, the dominant Movement for Multiparty Democracy (MMD) touted Chinese infrastructure projects in its political campaigns, making use of groundbreaking ceremonies to rally support for its candidates. However, after several violent encounters between Zambian miners and Chinese managers in the country's Copperbelt province, a deadly 2005 explosion in a Chinese mining explosives plant, and public opposition to competition from urban Chinese traders, opposition candidate Michael Sata was able to frame the MMD as a puppet of the Chinese. Tapping into anti-Chinese resentment among mining unions and displaced local traders, Sata overcame Zambia's unequal electoral playing field, melding disparate Chinese actors - such as the government in Beijing, independent Chinese traders and workers, and Chinese firms and investors into a unifying Chinese monolith, using this target to mobilize public support, unite a diverse rural-urban coalition and launch himself into the Presidency in 2011.

Throughout much of the continent, Chinese and other international investors have quietly made deals with local politicians to secure favorable access to African raw materials. A 2014 investigation of leaked documents, interviews and corporate records found that Jack Pa, a Chinese businessman, had constructed a shadowy organization - the Queensway group - which had secured tens of billions of dollars in secret deals. These dealings were concentrated in some of Africa's most corrupt and/or resource-rich regimes including Angola, Guinea, Zimbabwe, and Nigeria. The leaked documents from the Panamanian firm, Mossack Fonseca, known as the "Panama Papers," revealed the extensive use of secret offshore accounts to cover up the international investors' frequent use of bribes and political connections to secure access to oil, gas and mining rights and to avoid local taxes as well as labor and environmental regulations.

Such revelations have been circulated throughout African local media and social media networks, creating public pressure against secret deals for natural resource rights and encouraging greater public scrutiny of infrastructure projects. Of course, digital access and freedom have varied dramatically across the continent, ranging from the highly restricted networks of Ethiopia and the Gambia to the relatively open networks of South Africa and Kenya. More open digital environments have helped support digital activism and online-organized street demonstrations, whereas such activities have been constrained in closed environments, such as Ethiopia, subject to greater censorship. Following a global trend, incumbent rulers have attempted to regulate and control digital content by arresting users who publish sensitive and controversial content and for using keyword searches and other methods to monitor and censor communications on Facebook, Twitter, WhatsApp, and Telegram. The digital age has thus created uneven openings for new forms of political expression and activism, while also providing opportunities for opportunistic politicians to tap into underlying popular resentments and frame counter-establishment political platforms.

The digital age has thus created uneven openings for new forms of political expression and activism, while also providing opportunities for opportunistic politicians to tap into underlying popular resentments and frame counter-establishment political platforms.

Steve Hess is an Associate Professor of Political Science at the University of Bridgeport and co-author, with Richard Aidoo, of the book, *Charting the Roots of Anti-Chinese Populism in Africa* (Springer, 2015). Dr. Hess may be contacted at shess@bridgeport.edu

Populism in Eastern Europe: rise, decline or maintaining the status quo?

Interview with Dr. Tsveta Petrova
Columbia University

Is populism on the rise, decline, or status quo in Eastern Europe?

Like Jan Werner Muller and Cas Mudde, I understand populism as political movements and parties sharing an anti-establishment, monist and moralist ideology that is often combined with other ideologies. Examples of these ideologies include nativism on the right and socialism on the left. Populists thus depict society as divided into two homogenous and antagonistic groups: "the corrupt elite" and "the pure people" whose popular will ought to govern politics. In other words, populists polarize society and deny the existence of divisions of interests and opinions within "the people." Moreover, populists not only claim to be the only true representatives of "the people" but they also promise and practice serving them (or just buy off citizen compliance) by promoting some socio-economic distribution, that is, "mass clientelism." Given this definition of populism, there are currently only two populist parties in power in the Eastern European countries-members of the EU - Fidesz in Hungary and Law and Justice (PiS) in Poland. There are no populist movements in the rest of the region that appear as likely candidates for the assumption of power in the next few years. That said, some of the illiberal (opposition suppresion), nationalist (Euro-sceptic and anti-minority/ migrant), and distributive (anti-austerity and pro-social) practices used by Fidesz and PiS are popular in the region and unlikely to wane quickly.

In general, are there any significant differences between Eastern European populist parties and those in Western Europe, such as Marine Le Pen's National Party and Germany's AfD?

There are some interesting differences between the Eastern and Western European nationalist parties. First, in the Eastern European countries-members of the EU, we see not just right or extreme-right nationalism but also left nationalism. Most importantly, left nationalism can be observed among mainstream socialist parties in countries such as Romania, Bulgaria, and Slovenia. Second, few nationalists in these countries are currently truly promoting an exit from the EU–or its core current pillars–as a number of extreme Western parties are. This is because, at the popular level, a majority of the citizenry is still pro-EU. Moreover, at the elite level, there is recognition that EU funds are a key source of investment in the economy and of resources for crony networks. So, as long as these countries get meaningful EU funding, they are unlikely to exit the EU (even if they like to look as if they have more say in it).

Have populist movements in Britain (Brexit) and the United States (Trump presidency) had any effect on Eastern European populist movements?

I see more of a feedback loop. Especially in the wake of Europe's migrant crisis of 2015, the political success of some Eastern European populist (and nationalist) movements domestically and in Brussels has served to strengthen similar movements in the West, if not by example, then in numbers. Consider, for example, how Hungary's Fidesz took the initiative and helped give a prominent voice to movements and parties opposing Europe's refugees and migrants policies. Ironically, it's also the Eastern European migrants to Western Europe who will suffer as a result of the rise of Western nationalism. More broadly, Eastern populism has also exposed the EU's impotence in preempting and marginalizing such movements. The EU has served as their foil, kindling their popularity and has contributed to their survival through its cohesion funding policies. Brexit and Trump's rise to power are in turn emboldening similar governments to push forward with their illiberal and anti-EU agenda since neither the EU nor the US is perceived to have the will or standing to promote or even project liberal values. For example, many individuals in Eastern Europe agree with the counterfactual that had Trump not assumed power in the US, the current socialist-led government would not have sought to push back so quickly and so aggressively against the anti-corruption movement in Romania. Also, Fidesz would not have sought to restrict academic freedom in Hungary.

Jaroslaw Kaczynski of the Law and Justice party holds considerable power in Poland. What has his party, PiS, accomplished?

PiS has very quickly and decisively rolled back democracy in Poland by politicizing the constitutional court, the public media, the prosecution and the country's civil service. Most recently, PiS has restricted the activities of civil society and is looking for ways to change the electoral rules. These measures are being taken to help the party increase its grip on power at the local level in 2018 and to remain in office after the parliamentary vote in 2019. Although these political changes are relatively unpopular even among PiS voters, the government has managed to compensate the PiS base by significantly increasing social spending (hiking child allowances and minimum wages, providing medicine for the elderly, raising the threshold for tax-free personal income and lowering the retirement age). Over the long term, the negative political and economic costs of PiS' political and socio-economic reforms will likely accumulate. However, it is not yet clear if the opposition will be able and will be allowed to take advantage of the socio-economic ramifications to topple PiS.

As the EU progresses with negotiations with the United Kingdom concerning Brexit, what do you expect his voice to be?

Like many other Eastern European states, Poland will seek to guarantee the rights of its citizens in the UK, ensure the UK's future contributions to the EU budget (and thus EU structural funds) and strike a deal within the two-year negotiating period to avert a worst-case outcome on these two issues. Poland prefers that its diaspora remain in the UK since remittances from them assists in keeping a lid on domestic unemployment and generally supports freedom of movement within Europe. Preventing any reduction in EU funds is a top priority, however, given the country's disproportionate benefit.

What popular public sentiments in Hungary continue to support Mr. Orban?

Orban saw in the migrant crisis some domestic and international opportunities. These opportunities include 1) To arrest the rise of its main competitor, the far-right Jobbik and 2) To rollback Hungary's isolation at the EU level. Since the summer of 2015, the government has nearly monopolized public discussion on this issue. The center-left opposition has been so weak and divided that it has been unable to articulate an

> **...many in Eastern Europe (both at the elite and the popular level), believe that this populist wave represents a swing of the historic pendulum that will eventually swing back.**

opposing view. Moreover, the government has manufactured conflict to promote this incident as a key political issue and to widen the majority behind Fidesz' stance. Currently, around 3/4th of Hungarian say that migration is "a problem." More recently, Orban has been increasingly taking aim at a broader range of independent and foreign-funded NGOs and civic institutions in Hungary. Orban will seek to intimidate and discredit them, likely introducing a new law forcing NGOs to reveal funding sources, the prelude to a smear campaign that will paint them as subversive, foreign agents. This represents a rising trend towards outright political oppression, which may be applied more liberally to the opposition in the future. But such an approach carries greater risks for Orban as well, since this may prompt a greater backlash from voters or from the EU.

The Romanian government has been riddled with corruption allegations. How has this affected support behind the populist Social Democrats (PSD)? How will developments affect their democracy?

According to the polls, the impact on PSD's electoral support, on average, was limited. However, the impact of the PSD's actions on Romania's democracy will be significant if the government succeeds in its attempts to roll back, or at least halt the progress of the anti-corruption campaign. Corruption in Romania is still widespread and as a result, undermines the country's institutions and economic performance. Thus, corruption robs the citizenry of some of the benefits of the market-economy and democracy they so seek.

What do you see as the future of illiberal democratic populist parties in Eastern Europe?

If we look concretely at PiS and Fidesz, the popularity of both is currently declining. PiS is in a more tenuous structural position because of the relative strength of Poland's civic and political opposition. In both cases, however, many in Eastern Europe(both at the elite and the popular level), believe that this populist wave represents a swing of the historic pendulum that will eventually swing back. Perhaps, the pendulum will swing back soon, or at the latest, as the economic cycle turns and fiscal room for mass clientelism is constrained. As a student of regime-change waves, I tend to agree with this outlook. Still, the next liberal moment will not be a return to the previous liberal order given the significant popular and elite appetite for change, especially when it comes to liberal economic policies and political rights and entitlements. Consider, for instance, Eastern Europe's relationship with the EU, which for many in the post-communist region is the historic embodiment of these principles. The EU's eastern member states see themselves as second-tier members—in the eyes of their citizens, their standards of living have not converged with western standards as Eastern Europe has remained primarily a low-labor-cost manufacturing outpost of the West without a voice even on matters that are perceived as important. Popular support for larger domestic ownership of the economy, state support for the socioeconomic welfare of the region's citizens, and more national sovereignty amid rising disappointment with Brussels fueled the rise of populism in the east and made these countries vocal, if not united on an array of EU-related issues—including the migrant crisis, Brexit, Russia, and the EU's energy and climate policy. This will likely become the new normal.

Tsveta Petrova is currently teaching at Columbia University's MA Program in Modern European Studies. She received her Ph.D. in political science from Cornell University in 2011 and then accepted post-doctoral fellowships at Harvard University's Davis Center and then at Columbia University's Harriman Institute. Her research interests lie at the intersection of domestic politics and international relations in Europe. Her book on democracy export by new democracies, *From Solidarity to Geopolitics*, was published by Cambridge University Press in 2014.

Media, Web, and Democracy: populist and post-populist Europe in the mirror of the Italian experience

Professor Giovanna Campani
University of Florence

Introduction

In the European political debate, where the media-populism relationship has become a key topic, Italy represents an interesting case study: two main political forces -- defined as "populists" by mainstream media[1], "Forward Italy"/The People of Freedom (*Forza Italia, FI/Popolo delle Libertà,* PdL), the party invented by Silvio Berlusconi, and the Five Stars Movement (*Movimento 5 Stelle*, M5S), founded by the comic-turned-politician Beppe Grillo and the web strategist Gianroberto Casaleggio -- owe their successes to their ability to gain mass support through television in the first case and the Internet in the second. In 1994, 2001, and 2008, Berlusconi won the general elections; in 2013, the Five Stars Movement, running for the first time in a national electoral competition, gained just under 9 million votes, sending 163 Deputies and Senators to the Italian Parliament.

Scholars such as Mazzoleni (1991), Umberto Eco (2007)[2], and Fella and Ruzza (2011) used the term "media populism" in order to grasp the Italian experience during the years of Berlusconi's power. More recently, scholars (Newall, Giovannini, 2016[3], Tronconi, 2016) have analysed the link between the rise of the Five Stars Movement and the web. Internet strategist Gianroberto Casaleggio realised that, with the help of social media, he could grow Beppe Grillo's loyal fan base into a political movement. Beppe Grillo's blog was founded in 2005. Nowadays, Britain's *Sunday Observer* magazine ranks it as the ninth most influential blog in the world (Tronconi, 2016, p.42).

Focusing on the Italian experience, this article develops three contemporary debates: the ubiquity of mass media in the construction of the political communication; the possible strengthening of democracy, namely in the perspective of direct democracy, through the Internet; and the crisis of mainstream parties in the midst of the European Union crisis.

Neo-populism in Italy: The Rise of Silvio Berlusconi and the Media Factor

In contrast to other European countries such as Austria[4] or France, Italy's "populist" parties did not rise from the heritage of neo-fascist, neo-Nazi, or far right experiences. Neo-fascism, a constant presence in the Italian political landscape since World War II[5], did not play any role in the formation of the "neo-populist" experiences that developed since the 1990s (Campani 2016): the ethnic regional Northern League, the "media populism" of Silvio Berlusconi, and the anti-establishment Five Stars Movement. Among these three forces, only the Northern League, whose founder Umberto Bossi came – paradoxically - from the left, has finally placed itself at the far right, establishing an alliance with the Front National of Marine Le Pen. "Forward Italy" has always defined itself as "moderate" and center-right. Mildly Eurosceptic[6], Berlusconi tried to be accepted by the "European establishment" and succeeded in making his party a member the European People's Party Group in the European Parliament.[7] The Five Stars Movement rejects the right/left dichotomy, considering that both have betrayed the citizens, aiming the "disintermediation" of the Parliaments and the people's rule by direct democracy -- all through a simple click-of-a-smartphone app.

The emergence of the Northern League and Forward Italy followed the dissolution of the traditional mainstream parties, namely Christian Democrats and Socialists, that were swept away by corruption scandals in 1992, in the midst of the post-World War II order collapse (fall of the Berlin Wall and end of Soviet Union) and the transformation of the Italian economic and social structure (shrinking of the working class, growth of self-employment, and small/medium enterprises). The passage from the "first" to the "second" republic saw the confrontation between a new, recomposed center-right, gathered around Silvio Berlusconi, which included the Northern League, and a new, recomposed, pro-European center-left, gathered around Romano Prodi's The Olive Tree/Democratic Party (*L'Ulivo*), which rose from the ashes of the Communist Party and the left-oriented stream of the Christian Democrats.

Definitely a populist force, the Northern League used traditional forms of political communication and mobilization such as gatherings, feasts, and mass demonstrations (Diamanti 1993; 1996). Silvio Berlusconi's political trajectory is, on the contrary, linked to the media. In 1994, when the general election was announced, he sent a nine-minute video speech to his own TV channels[8], proclaiming that he was "taking the field" as leader of a new political force, "Forward Italy." Serving as prime minister for a few months, Berlusconi governed again between 2001 and 2006. Briefly defeated by Romano Prodi in 2006, he was re-elected in 2008 after the Prodi's coalition collapsed, and was forced to resign in 2011. This was due to a combination of popular rejection, internal defections, and international pressures – namely by the European "establishment" (the Franco-German alliance of Angela Merkel and Nicolas Sarkozy, plus the pressure of the Commission Chef Barroso). The main reason why Berlusconi was evicted was the government's management of the economy: the unelected government of the ex-European Commissioner Mario Monti imposed austerity policies in Italy (Andrews, G. 2005).

Marco Tarchi (2008), one of the most astute Italian political scientists, argues that Berlusconi's populism was a question of style, while his program had conservative connotations and could not be considered populist.[9] Other scholars, however (Lanni 2011), argue that this style of political communication revealed a shift in the idea of democratic government: While the Christian democrat, socialist or communist politicians needed their parties' support, Berlusconi communicated directly with the people through the media.

According to Mazzoleni (1999) and Fella and Ruzza (2011), this type of communication is part of the "media factor" -- the use of the media to conquer votes and to govern. The "media factor" touches one of the core principles of representative democracy: the freedom and independence of the media. As owner of three televisions, newspapers, and magazines, Berlusconi represented a conflict of interest with the idea of a pluralistic democracy that had shifted towards an illiberal democracy.

In the 1990s, Berlusconi was an anomaly in Europe; nowadays, the independence of the media is threatened in many European countries, such as by restrictions imposed by the illiberal democracies in Eastern Europe's Hungary and Poland.

The Media Factor and Media Populism

The debate on the "media factor" and "media populism" is not specific to Italy -- the ubiquity of the media in the construction of political communication – the media factor – is a general phenomenon all over the world. Mazzoleni (2003) defines the "media factor" as "the complex of processes that are typical to mass communication and especially of the news media in democratic environments, which interact with and affect (or are affected by) political processes to different extents and with different effects." (Mazzoleni 2003: 1–20). According to Mazzoleni, there is a level of complicity between the "news media" and political populism. The increasing commercialization of the news industry intensifies the natural search of the media for mass audiences, as well as their craving for sensationalism, scandal, and conflicts. The consequence is a close connection between media-originated dynamics and the rise of populist sentiments, fuelling populist movements – a case of "media populism" (Fella, Ruzza 2011).

Berlusconi fully exploited these dynamics. Thanks to his political connections, he succeeded in breaking the state's monopoly of network television, broadcasting nationwide first one, then three, channels that progressively forged a new popular sub-culture, a mixture of neo-liberal individualistic values (quiz shows as individual success and easy money), sexism (the exploitation of pretty naked girls), and consumerism, opposing the left-oriented culture of the Seventies with its dreams of social equality, political engagement, and rejection of consumerism.

Erik Gandini's 2009 documentary film *Videocracy* details the Italian experience of intellectual decay since the mid-1980s: television programs that replaced any cultural impetus and inculcated a social ideology that describes success – measured by a person's presence on TV – as the main goal of human fulfillment. Control of the media and the hegemony of the popular sub-culture were the backbones of the electoral success of Silvio Berlusconi.

Interviewed by D. Solomon, Umberto Eco defines "media populism" as appealing to people directly through the media; a politician who can master the media can shape political affairs outside of Parliament and even eliminate parliamentary mediation (Solomon 2007). Eco adds that, "From '94 to '95, and from 2001 to 2006, Berlusconi was the richest man in Italy, the prime minister, the owner of

> *Berlusconi's media populism is not just a question of style; it introduces the direct relationship between the leader and the "people" – through the media – weakening representative democracy.*

three TV channels, and controller of the three state channels. He is a phenomenon that could happen and is maybe happening in other countries. And the mechanism will be the same" (Solomon, 2007).

According to Eco, Berlusconi's media populism is not just a question of style; it introduces the direct relationship between the leader and the "people" – through the media – weakening representative democracy. Daniele Albertazzi and Duncan Mac Donnel (2008) define Berlusconi's populism as "the claim that sovereignty, rights and values of a homogeneous and virtuous people are under threat from a set of a corrupt and incapable elite" and that the leader can solve the problems, overcoming the traditional parliamentarian structure, even at the price of reducing the checks and balances of power. Berlusconi's fight against the judges and their autonomy is a manifestation of this claim.

However, Berlusconi's attempts to introduce aspects of an illiberal democracy, reforming justice, and institutionalizing his power on the media, failed. From a "centrist neo-populist" position, he could govern Italy for several years, while the European far right "populist" parties remained at the fringe of the political establishment, offering at most external support to conservative governments.

The Web and The Rise Of Beppe Grillo's Five Stars Movement

After the predominance of the "Videocracy" television culture, the arrival of the Internet in the late 1990s broke the media monopoly dominated by Berlusconi and introduced a new approach to information by public opinion.[10] Web political activism raised interest among scholars working on social movements as Andreatta (2002) and Della Porta (2005; 2006; 2007), who explored the structures of mobilization via Internet in the case of the alter-global or no-global movements. Della Porta (2007) raises issues of the role of the Internet in political socialization, identity construction, and capacity to mobilize in respect to special offline-events. The interaction between offline and online political activities is a major question for Web analysis.

The Italian social networks opened new possibilities for political mobilizations such as the Purple People (*Popolo Viola*) that, in November 2010, used Facebook to gather two million people to demonstrate against Silvio Berlusconi. The success of these mobilizations showed that a post-internet order was beginning and that the old mainstream media were losing their influence.

In 2009, Beppe Grillo and internet strategist Gianroberto Casaleggio founded the Five Stars Movement (*Movimento 5 Stelle*, M5S) as a web-based organization. Literally, the five stars in the movement's name represent the five issues it cares most about: public water, sustainable transport, sustainable development, the right to internet access, and environmentalism. All these topics were raised by Beppe Grillo in his theatre shows.

The movement is fueled both by disgust with the political class and the promise to launch a process of participation from the bottom, opening the debate on direct democracy through the web and internet-based deliberative processes (Gagliardone 2013). The M5S is an outspoken advocate of the potential role for social media to revolutionize Italian and European politics. Rejecting the idea of a traditional party structure, the structure of the organization functions through the proliferation of the "Meetup"

- an app[12] that allows people to create their own group and meet people nearby who share the same interests.

The Five Stars Movement "Meetups" gather the friends of Beppe Grillo who meet locally in order to discuss topics proposed in the blog. According to the latest data, there are 1,262 Meetups all over the world (including three in the United States and one in Argentina) with 164,722 members. There is no previous selection in order to become members of a Meetup. The selection takes place in the platform that is linked to Beppe Grillo's blog.

The use of the media (television and the web) for a political career pushed some scholars such as Lanni (2011) to establish a parallel between Berlusconi and Grillo, pointing out the differences and the similarities. The differences lay in the fact that the M5S mobilizes in a horizontal manner via the Internet – through the blog and the meet-up system - while Berlusconi established a vertical relationship through television. The similarities are the centrality of the charismatic leader, the disruption of the mechanisms of representation and mediation, and the rejection of traditional, organized parties – all aspects that have to do with a new role attributed to the media. Both leaders have developed a specific style of political communication by using the media and attacking it at the same time. Berlusconi, who, besides television networks, owns daily newspapers and magazines, dislikes journalists. So does Grillo: the Five Star movement elected MPs in 2013 who were prohibited from participating in TV talk shows for a couple of years.

The key that explains the interconnection between these two forms of populism is the concept of "disintermediation" applied to politics. New web technologies allow users to perform certain functions that previously required the mediation (and work) of other entities. Before the Internet, it was necessary to use a travel agency to buy a plane ticker, but today you can use your computer directly to save time and energy. Similarly, while the pre-Internet public participated in politics via a party or an association, today's public can just as readily use blogs, social networks, and/or virtual podiums in order to circumvent traditional organizational methods. However, this has the potential to create several problems: the need to change the function of a "meetup" that is infiltrated by people who have only career interests, or worse, are sent by other parties to create problems to the Five Star Movement.

Attentive to the role of the media, Lanni (2011) suggests the possibility of a "progressive populism." According to the scholar, if European populism is generally right wing, the Five Star Movement might represent a progressive populism, raising topics like ending corruption, reducing the costs of politics, and ensuring universal income.

According to Adinolfi (2012), the Five Star Movement uses the symbolic power of the Internet to gain legitimacy, but it has not really exploited the potential of the Web: The "Rousseau", the 5 Star Movement's Operating System that allows the signed-up members to participate in M5S activities by doing such things as drafting laws and voting to choose electoral lists and deciding on positions inside the M5S, is still used by a limited number of people. As an example, the number of certified participants voting on the energy program of the Five Star movement was 21,867.[13]

Adinolfi suggests that Grillo has – so far – promoted a kind of fetishism of the Internet, rather than a real willingness to learn from the logic of freedom, openness, and decentralization of the Internet to promote new and innovative forms of participation. Adinolfi (and partly Lanni) consider the web as such an instrument of democracy, but they do not think that the Five Stars Movement has - so far - developed the right instruments.

Post-populist Italy, Post-populist Europe: The Crisis of the Mainstream Parties

There is no doubt about the role of the Web in the rise of the Five Stars Movement. It shouldn't however be forgotten that the Five Stars Movement combines the use of the Web with traditional practices – gatherings, meetings, door-to-door – and can count on the charismatic presence of Beppe Grillo who, especially in the past, multiplied the speeches and the performances. Moreover, this anti-establishment political force promised to fulfill the "unsatisfied social demands" -- ending corruption, improving the economy, fighting unemployment -- of an Italian society shaken by several years of crises.

In the book *On Populist Reason*, Ernesto Laclau theorizes that populism begins when unsatisfied social demands become increasingly accumulated in a society (Laclau 2005: 73). Populist leaders identify with the inability of the system to absorb them and articulate the existence of a group by constructing an equivalent chain between the differential characters of the various segments of the society (Laclau 2005: 74).[14] These "unsatisfied social demands" vary by country. The political answers can also vary: populism constructs the people as a collective actor to confront the existing regime. Populism is one form of politics among others -- it can be right-wing populism or left-wing populism. Left-wing populism can construct an alternative narrative to neo-liberal hegemony. This analytical grid corresponds to the Italian case.

The rise of the Five Stars Movement – reaching twenty-five per cent of the voters in the national election in 2013 – and winning local elections in Rome and Turin and other towns in June 2016 - followed the discredit striking the entire political system, in the shadow of continuous corruption scandals, the worsening of the citizens' conditions, and the economic crisis. It emerged from the prevalence of "unsatisfied social demands." In surveys conducted in March 2017, the Five Star movement was credited with thirty-five percent of the votes (five more than the Democratic Party) and is now in the position to achieve gains in the next Italian electoral elections.

Looking at the expansion phase of the Five Stars Movement, we can see how the electoral success of 2013 corresponds to a specific political period. After the fall of Berlusconi in November 2011, via the Monti Government, the Italian parties (the center-right and the center-left) copied the European model of consensual governance based on the European neo-liberal dogma and accepted subordination to the EU. Imposed austerity measures contributed to a worsened Italian economic situation and an increasingly impoverished country.

The rejection by Italian voters of the Monti government and the party he had created (*Scelta Civica*), and the rise of the M5S were some of the first clear signals sent to the European Union after the crisis of 2008.

After 1945, the European leadership/establishment – the main parties, Christian Democrats/Social Democrats – discounted nationalism and sought increasing European integration, but they also guaranteed the citizenry protection from economic vagaries via the welfare state. The post-World War II order knew different phases. A new order took place after the fall of the Berlin Wall and the adaptation of mainstream parties to neo-liberal hegemonic ideas. The elites pushed to accelerate the integration of Europe through a shared currency, the Euro. We can argue that the elites domesticated the political dimension through the consensus around the uncontested hegemony of the neo-liberal thought and the growing role of a supranational entity – the European Union. This political consensus blurred previously exitsing distinctions bewteen left and right philosophies.

This order is now collapsing. Far-right parties are constantly growing, as in the case of Austria and France. All over Europe, far-right parties are becoming too big to ignore or to simply dismiss as "populist." Populists are no longer "fringe parties" -- they are at the core of the political debate in such critical settings as the next French presidential election: Marine Lepen won twenty-two percent of the vote after the first round.

The collapse of the old order takes different paths – not only the one represented by the growth of the far-right parties. New political parties are appearing, trying to reinvigorate democracy, as, in Spain, Podemos, and the anti-establishment party, arisen from the Indignados movement, Syriza in Greece, or the Five Stars Movement in Italy.

Italy – considered an "anomaly" in the 1990s – was the precursor of processes that are taking place all over Europe, as well as the disaggregation of the mainstream political parties. Old parties like the socialist Greek Party are disappearing; others, like the Socialist French Party, are weakened.

This order collapsed under the weight of the economic crisis in 2008. The creators of the European Union had promised to bring peace and prosperity, but, because of internal bad functioning and contradictions, they instead brought debt, despair, and disintegration. The Eurozone has become a disaster of quite staggering proportions, as levels of youth unemployment remain above twenty percent, and as high as forty-five percent in Greece. It is all the more astonishing for being both predicted and avoidable. The EU has no solution to the migration crisis even though it was the foreseeable consequence of a free-travel area that had no protection for its external border.

The blurred borders between right and left opened space for new political formations that, in a time when the traditional form of organizations represented by the parties are going through a deep crisis, exploit the new media technologies.

Given the most recent developments, there is no analytical and political value in doing an amalgam of "populist" and "radical" parties from the left to the right, whose worldviews and policies are totally at loggerheads, simply because they do not accept the neo-liberal dogma.

As we have seen, Italian "populism" emerged as result of a deep crisis of the parties system that, at the time, had no equivalent in the rest of Europe. Berlusconi offered a "populist" answer through the personalization of politics, using the media for a new style of political communication.[15] Moreover, being rejected by half of all Italians, Berlusconi channelled unsatisfied social demands into a personalized conflict between himself and the center-left. When the two contenders appeared to be unable to respond to the unsatisfied social demands, a new force appeared: the Five Stars movement. The same process has taken place in Greece, with the rise of Syriza, and in Spain, with the rise of both Podemos and Ciudadanos.

Should we call this process a shift towards "populism", as mainstream media and scholars do? We could, but we should look at the variety present in the so-called populist galaxy and consider populism just as a political form that should not necessarily raise contempt (Laclau 2005).

In respect to the entirely negative interpretation of populism as a demagogic, anti-system, unrealistic trend, I argue that we are entering into a phase that could be defined as "post-populism", where the so-called populist parties are presenting new political offers – both at the right and the left of the political spectrum – in order to transform the present order. And they find the support of the citizens.

Conclusions

The media played a crucial role in the Italian "populist" experience; they were an instrument of political action and they transformed the political communication, but the roots why these new "populist parties" emerged were social, economic, and political. The media alone has not produced "populism"; populist leaders have themselves manipulated the media.

The Italian experience preceded common European trends. The Italian "anomaly", represented by Berlusconi's "media populism", has been a precocious sign of a deep crisis touching representative democracy that European citizens perceive as dominated by oligarchical and technocratic elites aiming to construct firewalls against "the multitude." The 2008 economic crisis has reinforced this perception, placing the European Union at the core of the popular rage.[16]

Europe is experiencing a long transition from a previous political order towards a new one, characterized by the formation of political forces that are breaking with the old "consensus", namely the uncritical support for the European Union and the European neo-liberal dogma for the management of the European economy.[17] The paths to change the present situation diverge deeply: some new political forces lean towards illiberal democracy, proposing the renewed role of an authoritarian national state (this is the "Putinian model" represented by Orban in Hungary); others push towards new forms of direct or participative democracy, like the Five Stars Movement in Italy and Podemos in Spain.

To define all these forces as "populist", without making distinctions between their worldviews, does not push the analysis far enough. A critical approach must reject a broad definition of "populism" that embraces parties and movements whose common feature is the rejection of the cartel-like power of the political elite (Jones 2007) but whose worldviews and policies are totally at loggerheads. The media is a strong instrument to gain political influence. They are at the origin of new forms of political communication and may be a support for new ideas about legitimacy based on popular consent.

However, their role should not be overestimated: the political use of the media co-exists with more traditional practices (meetings, demonstrations, speeches, door-to-door campaigns); more importantly, what is at stake in Europe is not the form, but the contents of the political battles: world views, ideas on democracy, national sovereignty, and the basis of political legitimacy – popular consent or oligarchical rationality.

What is at stake cannot be reduced to a confrontation between "populist" insurgency and "mainstream" democratic parties: the present political phase should more appropriately be defined as "post-populist". In fact, the "populist" insurgence against the establishment succeeded to impose its topics in the political agenda – as Brexit demonstrates. This happened not because the "populists" did a better job at propaganda (through media), but because they raised real problems for the European populations – such as identity, sovereignty, competing economic models, and the role of the EU. In many European countries, the "populists", having conquered a large part of the electorate, are no longer at the fringe. The issues raised by the so-called populists have been incorporated in one way or another in the general debate. We can say that Europe, too, is entering into a post-populist phase, characterized by growing uncertainties.

Giovanna Campani is professor of Intercultural Education and Gender Anthropology at the University of Florence. Besides populist movements, which has become a major field of study for her, her main research field comprises intercultural education, comparative pedagogy, studies on migrations and gender, social inclusion/exclusion, migrant integration in educational systems and intercultural activities, refugees' protection, trafficking in human beings, female married migrants, processes of migrants' labour insertion, and unaccompanied minor migrants.

She has recently edited two books: *The Rise of the Far Right in Europe* (2016) with G. Lazaridis and A. Benveniste (Palgrave) and *Understanding the Populist Shift* (2016) with G. Lazaridis (Routledge).

CYBER SECURITY

Cyber Threats and Cyber Policies

Interview with Dr. Peter W. Singer
New America Foundation

What are your main concerns regarding cybersecurity currently?

There's so much happening from new technology and new dilemmas, but unfortunately, there's something I just can't get past, which is that we just had the most important cyberattack in history, and a large part of our political system just wants to whistle by and forget it. We had Russian cyberattacks on a wide variety of American political organizations, individuals of both parties; as well as non-governmental groups, from think tanks to universities, to governmental sites like the Pentagon email system. This was not a one-off event. They were identified by five different cyber security companies as Russian in origin and also officially identified by the U.S. government as such. Also, belatedly and begrudgingly, the attacks were admitted by the current U.S. President to have been Russian in origin.

Yet not much has happened in reaction to this, other than the stop gap sanctions put into place by the Obama Administration, which are at risk of being lifted by the Trump Administration. This is big. It's not just a campaign that's hit the U.S., it has also hit multiple allies of ours, and it's ongoing. So again, there are lots of other things that we can talk about in this space, but it's hard to ignore that many people want us to ignore this cyberattack.

After the attacks, Senator McCain said, "the American response was totally paralyzed." What should be done to better thwart and respond to these kinds of attacks?

It is interesting that a number of congressional leaders, not just Senator McCain, but both the Speaker of the House and the Senate Majority Leader attacked the Obama Administration responses as too little, too late. They were quick to make that criticism, and, quite frankly, they were right. But a test of their sincerity is whether they will back these words with actions by turning these sanctions into law and strengthening them further. The important part of turning them into law is that it makes it harder for Trump to set them aside, as both he and his aides have made clear they'd like to do. Strengthening sanctions could aid restoring and bolstering deterrents in this space. If Congress actually acts, it would show Putin that the party of Reagan and Eisenhower is willing to stand up to Moscow rather than shower it with praise.

So, what else can we do? It's not about punishment. It's about seeking to find pressure

..we just had the most important cyberattack in history, and a large part of our political system just wants to whistle by and forget it.

points to influence future action. The overall weakness of the Russian economy as well as its oligarchic structure, are choice leverage points. It is notable that the U.S. is being bullied about by the world's thirteenth largest economy and falling. Russia's economy is the equivalent of Spain. Targeting financial assets of Putin and his allies, particularly those held outside the country in real estate and tax shelters, would be something I would expand. Outing these assets should also be the target of activities beyond sanctions. One of the things that authoritarian regimes fear is what they try to ban discussion of. The Russian regime's anger at the publication of the Panama Papers, which show just a very small portion of where its money was hidden around the world, reveals an area that could be exploited further.

The same twin goal of outing and defanging networks should also be applied to the financial and digital infrastructures that have been used to conduct these attacks. By outing them, you make them harder to operate in the future. But there's an important caveat here. It's not just about hitting back. You also can and should build up resilience, the ability to shrug off future attacks. This is known in deterrence theory as "deterrence by denial", that by making attacks less beneficial to the attacker, they are made less likely. What's important about building up our own resilience is that this would be of benefit not just against Russia, but any attacker, whether it's other high-end threats, like China, to low level threats such as cyber-criminals.

There are also all sorts of things that we could be doing better in building our resilience and almost all of them are non- or bipartisan. An example was, after the OPM breach, the Obama Administration identified a series of best practices from business that could be brought into government to aid cyber security. Best practices from business? That feels like a nice Republican talking point. Congress should be making sure that these things are actually being implemented. Another example would be, towards the end of the Obama Administration, there was a bipartisan commission of experts that sent out a series of action items. Again, bipartisan. Now, put those into place. Some people will say they want one or the other of these things. No, you do both. There's a lot more that we could do here. But, for the most part, significant parts of our political bodies are whistling past it.

A few years ago, China was perceived as the largest cyber threat to the U.S. Has that abated?

It depends on how you define largest. What gained such interest was a massive and in-your-face campaign of intellectual property theft that was targeting everything from government research institutions to private businesses. It occurred from the area of defense to soft drink companies, furniture companies, you name it. This was raised at the highest levels with China right before the bilateral meeting a year ago, and it was made clear that if it continued at that level, it would sink the upcoming leaders' meeting and sour American-China relations. Reportedly, the scale of that campaign, the in-your-face nature of it, has gone down. There are some other things going on within China, from reorganization of how its military and government conduct these operations to anti-corruption campaigns, that have been tied to that decline as well. So, the bottom line, by most accounts, is that it's gone down, but not disappeared.

However, this is a tool, a leverage point in China's back pocket that it could bring them back if it sees relations sour. As an example, President Trump placed a pretty inflammatory phone call and series of tweets related to Taiwan right after he won the election, whereby Beijing sent signals of its displeasure by doing things such as kidnapping an American robotic submarine in the South China Sea and sending bomber flights around Taiwan. There's a similar response in their back pocket, which is to ramp back up the level of cyberattacks.

Let's switch to cyberterrorism, a topic many people are concerned about. For example, potential threats to infrastructure. Do you think those general fears are perhaps overblown?

Yes and no. The narrative of cyberterrorism is something that has had an outsized influence compared to the actuality of it. And let's be clear here. There have been over 50,000 mentions of "cyberterrorism" in some way, shape or form. But, there have been zero actual incidents of it, according to the FBI definition of cyberterrorism. Cyber terrorism is not terrorists using the Internet; it is actually using it to cause physical damage, death and destruction. If spreading propaganda was terrorism, a terrorist sending a letter would be "postal terrorism." But no, it's the terrorist sending the letter bomb that makes it postal terrorism. Right? Same thing here. So we've not actually seen any incidents of actual cyberterrorism yet despite all the stories.

This doesn't mean it is not a risk. It doesn't mean that it won't happen. It will. It will happen because of the clear interest in it and the lowering of barriers to entry, particularly as we move more and more to the Internet of Things, as we expand from using smartphones and laptops to also using smart cars, smart power grids, and smart medical devices. It's not just that the landscape of potential targets grows from roughly the 7 billion things that are linked up to the Internet right now, to the 50 billion things that are going to be online in a couple of years. It is also that, when you attack and gain access to "things," like a car, like a power grid, like a refrigerator, you can cause physical change in the world. Therefore, different kinds of risk are created than if someone stole your email. If you can pump the brakes of a car remotely, it's a lot different impact than being able to steal the financial information of who bought the car. The point is, there is a very real risk here. But again, too much of the discourse has been stuck on "cyber 9/11" and "cyber Pearl Harbor" bumper stickers that haven't been all that helpful.

On a lower scale, do you think that not enough attention is being paid to simpler cyber security risks that are potentially encountered with everyday activities, things like phishing, shoulder surfing, human factor risks?

Clearly we would be in a much better space if we just had a minimal level of cyber hygiene. By saying "we", I mean everything from individuals to national security at-large. The breach at the DNC is a great illustration of this, the "what if" that could have taken us in a very different history. But what I find fascinating is that we still don't teach these cyber security basics the way we should. And this applies again everywhere. For example, business executives regularly make cyber security decisions, everything from their own individual cyber hygiene to making decisions for their company on how it's going to invest in their space. Yet, MBA programs don't teach it the way they teach courses in ops, org behavior, finance and the like. Where if you're in an MBA program, even if you're not going to go into ops, or if you're not going to go into accounting, you still get the basics. We don't get the same coverage for cyber security, even though it will be a manager's responsibility.

This is important all the way down to our kids, given the massive amount of time they spend online. But, for the most part, we don't teach them how to protect and secure themselves online.

I like that notion of hygiene as a parallel. It's something that everything from parents to schools teach, because it's both protective of those that you love, but it's also protective of society at-large.

How do you see cyberwar capabilities affecting future conflicts?

It's not just the future; it's the reality of present day conflict. Just look at Russia versus Ukraine or ongoing events in Syria and Iraq. There is now a conflict that's played out not just on land or in the air, but also in cyberspace. What's interesting about it is, as the Russia/Ukraine episode reveals, is that the most consequential cyber parts of the conflict can happen before the real physical conflict begins. To put a little more flesh on that, Russia owned, both literally and virtually, Ukraine's communication networks before the first troops crossed the border. Because Russia did, it was able to have an almost paralyzing effect on the Ukraine in the first couple of days of the conflict. It was able to control and restrict the flow of information.

What we've seen in the Syrian and Iraq Wars is everything from online recruiting and propaganda to using cyber means to gain intelligence for use in physical targeting – "Where is someone actually located in the world, so I can drop a JDAM (Joint Direct Action Munition)." Cyber has become a front in much the same way battles in the air did a hundred years back. That will be the case moving forward, whether the adversary is a military actor or a state actor.

What about criminal activity through avenues such as TOR, the darknet?

There's a very active and vibrant ecosystem that supports criminal activity. Some of it is happening in dark markets and some of it happens quite out in the open. There are two projects here [at New America Foundation] that are interesting. One looks at how these criminal marketplaces operate in the dark web. What we found is fascinating but also a bit unsurprising; like in regular crime, they often center around language. For example, Russians tend to work with other Russians, Indonesians with other Indonesians and the like. There's a global marketplace but it actually breaks down into little subsets. Like other markets, there's lots of specialization, so it's not one person who does all things, but one person is very good at one particular role, and you bundle these different skill-sets together if you're conducting a campaign.

But again, that isn't just happening in the dark. It's actually happening in the open. There's an interesting study from a couple of months back concerning cybercrime advertising on Facebook. For example, you can go on Facebook right now and find forums for everything from botnets to rent to buying weapons in the Middle East.

We started out touching on legislation. Providing legislation that can handle rapidly evolving and expanding technologies is quite a challenge…

The challenge is that it's not the technology; it's the politics of it. There's a wide range of things that could be done that are politically difficult to accomplish right now. For example, creating legislation requiring companies to meet NIST (National Institute of Standards and Technology) standards and the like.

Where I see one of the more interesting parts of this moving forward is going to be the cyber insurance marketplace. What can government do to encourage its growth, which would allow more marketplace solutions? And one that would be more flexible and dynamic, where insurance companies are going to be able to figure out what they think is best for their coverage, and then companies are incentivized to meet that. I think we'll be in a much better place if we can create more incentives for building out this marketplace. There's lots of discussion about those incentives, but that to me is where we'll see more coming together than just government saying, "This is required." I'd love to see certain things required in terms of standards and insurance, but that's not politically going to happen right now.

There's a similar question around the issue of information sharing, and that, again, is not a technical question. It's more a question about liability. I think we've gotten better but there's still a ways to go.

Peter Singer is a strategist and senior fellow at New America. The author of multiple award-winning books, he is considered one of the world's leading experts on 21st century security issues. He has been named by the Smithsonian Institution-National Portrait Gallery as one of the 100 leading innovators in the nation, by *Defense News* as one of the 100 most influential people in defense issues, and by Foreign Policy magazine to their Top 100 Global Thinkers List. His books include *Corporate Warriors: The Rise of the Privatized Military Industry; Children at War; Wired for War: The Robotics Revolution and Conflict in the 21st Century; and Cybersecurity* and *Cyberwar: What Everyone Needs to Know*, which was named to both the US Army and US Navy professional reading list. His most recent book is *Ghost Fleet: A Novel of the Next World War.*

Singer is a contributing editor at *Popular Science* magazine and the founder of NeoLuddite, a technology advisory firm. He has worked as a consultant for the US military, Defense Intelligence Agency, and FBI, as well as advised a wide-range of technology and entertainment programs, including for Warner Brothers, Dreamworks, Universal, HBO, and the video game series Call of Duty, the best-selling entertainment project in history.
He is a member of the US State Department's Advisory Committee on International Communications and Information Policy. His past work included serving as coordinator of the Obama-08 campaign's defense policy task force, in the Balkans Task Force at the Office of the Secretary of Defense, and as the founding director of the Center for 21st Century Security and Intelligence at The Brookings Institution, where he was the youngest person named senior fellow in its 100 year history.

NATO Cyber Challenges

Dr. Alexander Crowther
National Defense University

The North Atlantic Treaty Organization (NATO) is the most successful military alliance in the world, having achieved what had previously been impossible: create the environment for over 70 years of peace on the European mainland. An organization of the Cold War, NATO evolved in the decades since the fall of the Berlin Wall.[1] However, as the world continues to change, so must NATO. One recent challenge that NATO faces is the cyber environment. However, this same cyber environment also provides NATO with opportunities. Which will prevail in the end? Will NATO be undone by opponents wielding cyber weapons, or will NATO continue to adapt and successfully sail the cyber seas?[2]

The cyber environment seems to be all things to all people. Media tool, moneymaker, and existential threat are only three manifestations of the cyber environment. NATO, like the United States military, has defined cyber as a domain.[3] Regardless of definitions, to paraphrase Leon Trotsky: you may not be interested in cyber, but cyber is interested in you. A wide variety of states and non-state actors are active in cyberspace. Many of them do not agree with the values that NATO and the North Atlantic community stand for: democracy, human rights, free trade, and the rule of law. Because of this, NATO has had to involve itself in cyber issues.

NATO is an alliance of 28 states, headquartered in Brussels. It has a civilian component that could be called “political NATO” and a military component that could be called “military NATO.” Political NATO provides policy guidance, political oversight, and governance for the Alliance. It is headed by the North Atlantic Council (NAC), which consists of the heads of government of the 28 Allies. The civilian side also consists of the NATO Headquarters (the domain of the Secretary General), the Permanent Representatives and National Delegations, and the International Staff.[4] Military NATO consists of the Military Committee (made up of the Chiefs of Defense Staff; the U.S. member is the Chairman of the Joint Chiefs of Staff), the International Military Staff, and two commands: Allied Command Operations (ACO) and Allied Command Transformation (ACT).[5] ACO is also the Supreme Headquarters Allied Powers Europe (SHAPE), located in Mons, Belgium. ACO commands all NATO forces globally. ACT performs functions that do not pertain to operations: doctrine, training and exercises, education, interoperability, and lessons learned. It is located in Norfolk, Virginia, and is responsible for a widespread structure of schools and nationally-run centers of excellence.[6]

Because NATO is a political alliance, the policies of states sometimes significantly influence NATO decisions. Additionally, because NATO operates based on consensus, any state can veto any initiative, so the organization tends towards “lowest-common-denominator” decisions. This has impacted cyber decision-making in NATO. Because NATO is a defensive alliance, it refers to cyber issues in terms of "cyber defense."[7]

NATO has realized that cyber has been an issue for most of the 21st century.[8] The Alliance first placed cyber defense on the agenda at the 2002 Prague Summit. In the wake of cyberattacks on Estonia in 2007, the Alliance developed their first cyber policy, approved in January 2008. Events such as the cyberattacks on Estonia and the cyber-enabled military operations against Georgia in 2008 reinforced NATO's sense that cyber was important. At the Lisbon Summit in 2010, the Alliance adopted a new Strategic Concept, requiring the development of an in-depth NATO cyber defense policy. NATO integrated cyber into their Defence Planning Process[9] in April 2012. At the Chicago Summit later that year, NATO brought all of their networks under centralized protection and upgraded the NATO Computer Incident Response Capability (NCIRC) and formed the NATO Communications and Information Agency (NCIA) one month later. The NCIRC was fully operational by May 2014, and later that year NATO reached out to industry through the NATO Industry Partnership (NICP). NATO continued their outreach with a Technical Arrangement on Cyber Defence with the European Union (EU) in February 2016.

Later that year at the Warsaw Summit, NATO recognized cyberspace as a domain, joining air, sea, and land as areas where NATO would operate. NATO also signed a Cyber Defence Pledge[10], codifying NATO's way ahead vis-à-vis cyber. Later in the year, NATO and the EU issued a joint declaration, agreeing on a series of more than 40 measures to advance how the two organizations would work together.[11] NATO started 2017 with an updated Cyber Defence Plan and a roadmap to implement cyberspace as a domain.

The most important aspects of NATO cyber are[12]:

1) Cyber defense is part of NATO's core task of collective defense;
2) NATO has affirmed that international law applies in cyberspace;
3) NATO is responsible for the protection of its own networks;
4) Allies are and remain responsible for the protection of their national networks, which need to be compatible with NATO's and with one another's;
5) NATO reinforces its capabilities for cyber education, training, and exercises;
6) Allies are committed to enhancing information-sharing and mutual assistance in preventing, mitigating, and recovering from cyberattacks.

Because NATO is a defensive alliance, cyber defense has to be part of NATO's core task of collective defense. This focus on defense also bleeds over into cyber operations – NATO will only perform cyber defense.

Because NATO is an international organization, and "one core standard for all Allies" is the rule of law, NATO has affirmed that international law applies in cyberspace. This is very important, as several international players whose interests are inimical to NATO have claimed that cyberspace is like the "Wild West," where there is nothing except national laws. The United States and like-minded partners have argued that international law runs writ in cyberspace, therefore customary and treaty law are in effect. This means, among other things, that cyber espionage is espionage and cyber crime is crime. Thus, we do not need a whole new set of laws pertaining only to cyberspace. As NATO defends itself, it is logical that NATO is responsible for the protection of its own networks. However, because NATO is an alliance of nations, Allies are and remain responsible for the protection of their national networks, which need to be compatible with NATO's and one another's. Having interoperability amongst ally's communications electronics is only logical. Although it should go without saying, responsibility for their own national networks must be overtly stated to prevent another occurrence of the bane of NATO – security free-riding. If this statement was not inserted into NATO's cyber doctrine, some Allies might be tempted to short their own cyber security budget, comfortable in the knowledge that NATO would have to ride to the rescue in the case of a major cyberattack. Because different Allies have different cyber capabilities, NATO reinforces its capabilities for cyber education, training, and exercises to try to bring all Allies up to a certain level of capability. This reality is also why NATO mentions that Allies are committed to enhancing information-sharing and mutual assistance in preventing, mitigating, and recovering from cyberattacks.

Challenges

NATO faces several cyber challenges. The major challenge is cyber actors - both states and non-state actors. A secondary challenge is a lack of attention, prioritization, and resourcing. A third is the challenge posed by onwards-racing technology.

States, proxies that perform tasks on the behalf of states, terrorists, criminals, hacktivists, businesses, and even individuals aggressively pursue cyber operations daily. Because the barrier to entry into cyberspace operations is very low, virtually any groups or even individuals can set up their own cyber operations. In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Jason Healey identifies seven "Cyber Wake-up Calls,"[13] and *Real Clear Politics* developed a similar list.[14] When combined, they look like this:[15]

- Morris Worm - individual
- Eligible Receiver and Solar Sunrise - individuals
- Moonlight Maze - Russia
- Chinese Espionage - China
- Estonia and Georgia - Russia
- Buckshot Yankee – Unknown, probably state-sponsored
- Olympic Games/Stuxnet - Unknown, probably state-sponsored
- Titan Rain – China
- Operation Orchard – Israel
- Operation Aurora – China
- Iranian Retaliation for Stuxnet - Iran
- Flame – Unknown, probably state-sponsored

Note that three were performed by actors in China, three by unknown actors who were probably state-sponsored, two by individuals, two by actors in Russia, and one each by Iran and Israel. This serves to identify the broad array of actors that are operating in cyberspace. Some of these attacks can be traced to an IP address in a country, but the specific actor has not been officially identified in several cases.[16]

States tend to be the best-resourced cyber actors. Russia, China, the United States, and the United Kingdom could be considered the top tier cyber states. North Korea, Iran, Israel, France, Germany, and the Netherlands could be considered the second tier of cyber states. Proxies that support states perform many intelligence, operational preparations, or offensive cyber operations on behalf of their patrons. Proxies provide their state sponsors with deniability. Unfortunately for state sponsors, proxies are not always the most competent nor totally under control. States using proxies must balance the convenience and deniability of using proxies against the potential negative aspects of failure or triggering an adverse reaction from a target. Cyber crime cost the global economy $445 billion (USD) per year in 2015. It cost the top four (U.S., China, Japan, Germany) over $200 billion (USD).[17] Forbes projects that cyber crime costs will reach $2 trillion (USD) by 2019.[18] Hacktivists or independent non-state actors are also very active in cyberspace. These groups routinely deface or otherwise deny cyber capabilities belonging to their victims.

Cyber actors perform a certain series of operations. According to the U.S. Department of Defense, cyberspace actions include Cyberspace Defense, Cyberspace Intelligence, Surveillance and Reconnaissance (ISR), Cyberspace Operational Preparation of the Environment (OPE), and Cyberspace Attack.[19] Everyone should be performing cyberspace defense. Cyberspace ISR consists of actions taken to enter a system and discover valuable information about the system, such as identifying administrators and determining their credentials. OPE is where software is manipulated, allowing operators to return, or allowing operators to perform specific actions such as opening the sluice gate on a dam. Cyberspace attack is where a specific action is taken, such as transferring money or opening a sluice gate.

States, proxies, terrorists, criminals, and hacktivists perform these operations daily. NATO Secretary-General Jens Stoltenberg said there were 500 “dangerous cyberattacks” a month on NATO facilities in 2016, a 60-percent increase on the previous year.[20] States that oppose NATO efforts will perform ISR and OPE on NATO networks in case they ever come into conflict with NATO. Proxies will perform ISR and OPE on behalf of their state patrons, and will also attack NATO, allowing states to gauge NATO’s capabilities while protected from retaliation by hiding behind their proxies. Terrorists will perform ISR and OPE as well as conducting cyberattacks to deter or prevent NATO from striking them. Criminals will perform ISR, OPE and attacks against NATO personnel, seeking financial or other personally identifiable information (PII) to gain for themselves, or sell the information to those who want it, such as states and terrorists. Hacktivists will perform all three operations against NATO just because NATO is an international organization that supports state goals of the developed world. While NATO must defend all of their networks all of the time, attackers can perform operations whenever and wherever they want, choosing the time of their maximum advantage. As Russia currently seems to be the most likely combatant, and is also a first-tier cyber power, it represents the largest cyber danger to NATO. Russia was responsible for cyber operations against Estonia in 2007, Georgia in 2008, and Ukraine in 2014. Unfortunately, NATO, like everyone else, has proven unable to stop Russia. Sir Michael Fallow, the Secretary of State for Defence for the UK, said: “The NATO machinery is not geared up…It has not been fast enough in dealing with threats like terrorism or cyber… That's one of the areas in which NATO needs to be more agile. It needs to respond to cyber threats."[21]

The last cyber challenge that faces NATO is internal. Because NATO is made up of 28 states that have differing agendas, and voting requires unanimity, NATO is often prevented from taking action. As a trio of NATO Cyber researchers has commented:

> "NATO has shown little inclination to move away from its current purely defensive posture in cyber defence. At the political level, Allies remain reticent when it comes to discussing the options of using military (offensive) capabilities within a NATO setting. For most of them, cyber operations are generally still uncharted territory in which confusion abounds."[22]

When this author tried to engage individuals at NATO headquarters in Brussels in 2011 and 2012 to discuss offensive cyber operations, they refused to discuss anything other than defensive cyber operations. This internal issue has a magnifying effect on the challenges provided by external sources as discussed above.

Together, the internal and external challenges make it very difficult for NATO to thrive in the informationized societies of the 21st century.

Opportunities

Like the challenges, there are two sets of opportunities: those outside NATO and those within. Opportunities from outside NATO include their technical agreement with the EU, the NATO Industry Partnership, and cooperation with the Organization for the Security and Cooperation in Europe (OSCE). The European Union includes 22 (of 28) NATO members and has interests and values that closely mirror those of NATO. Indeed, an attack on any of those 22 NATO countries is also an attack on an EU country. EU-NATO cooperation also brings in 6 additional EU states as well as 6 additional NATO states, for a total of 34 countries, most of which are also in the Organization for Economic Cooperation and Development (OECD, the grouping of the most developed countries). The EU, like NATO, has a wide variety of the most developed tech companies in the world. Cooperation between the two can only be a plus. The NATO Industry Partnership is a vehicle to access those world-class companies that reside in NATO countries. NATO working with national Computer Emergency Response Teams (CERTs), multinational smart defense projects, and information sharing activities are several ways that NATO and industry cooperate. Cooperation with the OSCE allows NATO to coordinate with Russia, a member of the OSCE, and allows NATO to participate in the formation of global cyber norms, an effort that the OSCE participates in.

Opportunities within NATO revolve around the adaptations previously discussed. NATO has articulated a need to improve their cyber stance since the 2002 Prague Summit. The changes that NATO has made have been discussed above. What is important is the capabilities that have been created: from the development of the NCIRC, to the establishment of the NCIA, NATO has built capacity. Policy advances have occurred as well, from building a cyber defense plan to the recognition of cyber as a domain and the cyber defense pledge in Warsaw. This was important as NATO leaders agreed that a cyberattack could constitute an Article Five (i.e., collective defense) response, raising the prospect of war if an enemy state hacked a NATO country. Indeed, even the discussions within NATO have changed. During a recent conversation with several Deputy Permanent Representatives from seven NATO Allies, they revealed that the Alliance is actually discussing the utility of offensive cyber operations. The last cyber opportunity that NATO has is the strength of national cyber capabilities. NATO does not maintain nuclear weapons, but depends on the capability of the Allies who have nuclear capability (e.g., U.S., France, and the UK). This is also a paradigm that is useful for NATO. Several Allies possess offensive cyber capabilities that the Alliance can tap into.

Conclusion

NATO faces a number of challenges and opportunities in the cyber domain. A plethora of international actors who take advantage of low barriers to entry together with rapidly improving offensive cyber capabilities combine to provide a potentially lethal set of events. However, NATO has recognized the need to grapple with the challenges that cyber actors and capabilities provide. In response, NATO has reorganized, changed their policies, and developed partnerships with other potent cyber actors. Just as with the United States, NATO faces a future that contains potential peril, but also potential gain.

Glenn Alexander Crowther has lived overseas 13 times for a total of 25 years. He was personally selected to be a Counterterrorism Advisor for the US Ambassador to Iraq, a Political Advisor for the Multinational Corps-Iraq (MNC-I) Commander, and a Special Assistant for the Supreme Allied Commander, Europe. He is currently a Senior Research Fellow on NATO/Europe and Cyber Policy in the Institute for National Strategic Studies (INSS) at the National Defense University in Washington, DC. He has published in a variety of formats and locations, has experience teaching at the graduate level as well as a conference organizer and as a public speaker. Alex has a BA in International Relations from Tufts University, an MS in International Relations from Troy University, and a Ph.D. in International Development from Tulane University. He was also an International Security Studies Fellow at the Fletcher School of Law & Diplomacy. He has professional fluency in Spanish and capability in Portuguese. He specializes in NATO and Europe; cyber policy; strategy; Western Hemisphere issues; international development; insurgency/counterinsurgency; Joint, Interagency, Intergovernmental and Multinational (JIIM) issues and the Comprehensive Approach.

Deterrence of Cyber-Attacks in International Relations: denial, retaliation and signaling

Sico van der Meer
Netherlands Institute of International Relations 'Clingendael'

Introduction[1]

Deterrence of cyber-attacks by states or state-sponsored actors is becoming an increasingly important issue in international relations. The number of cyber-attacks in the world has grown sharply in recent years; especially instances of large-scale cyber espionage and cybercrime all over the world.[2] These types of cyber aggression cause primarily economic damage. Yet, in addition to economic consequences, such as weakening the competitive economic position of a state, cyber espionage in particular is also a security issue: it can be used by enemies to learn a great deal about another nation's security situation and discover potential weaknesses. Stolen information about, for example, military capabilities or vital infrastructure, could be used to cause harm through digital or non-digital means.

Cyber-attacks aimed at sabotaging or disrupting societies are far less common so far. Nevertheless, continuing digitalization is increasing the risk of more large-scale cyber-attacks aimed at disrupting societies and creating unrest, disorder, or even causing physical damage and victims. The worldwide number of devices and appliances that are connected to each other and to the Internet will increase to approximately 25 billion in 2020.[3] The greater the dependence on cyber technologies, the more vulnerable any society will be to cyber threats. A major cyber-attack remains a possible nightmare scenario. Much damage could be caused by cyber-attackers who succeed in sabotaging energy supply systems, chemical plants, nuclear installations, air and railway traffic control systems, hospitals, drinking water and sewerage facilities, payment systems, or a combination of these. In this sense, what applies to terrorist attacks also applies to cyber-attacks: although the probability of an attack may be relatively low in statistical terms, the impact of such an attack could be considerable. From that perspective, the trend of many states heavily investing in cyber forces is not reassuring.[4]

For states, the increasing threat of large cyber-attacks is not an easy challenge. Ideally, enemies are deterred before they actually launch a cyber-attack, so no damage is done at all. To deter cyber-attackers, their cost-benefit calculation needs to be influenced, leading them to conclude that the costs of launching a cyber-attack may be higher than the benefits. This article concisely discusses the main policy options that are relevant for deterring major cyber-attacks by other states or state actors. The options are grouped into three main categories:

1) Deterrence by Denial;
2) Deterrence by Retaliation; and
3) Deterrence by Signaling.

Deterrence by Denial

The most obvious way to deal with cyber threats is making such attacks more difficult for potential assailants by improving the security of cyber technology systems. One could label this as "defense" of a state's cyber domain, as "deterrence by denial", or as "passive deterrence" – passive because this policy is aimed at strengthening internal resilience, instead of actively influencing any actors from abroad. Deterrence by denial generally consists of technical defense measures, for example: multi-layered firewalls, advanced encryption, thorough authentication methods, so-called 'honeypots,' and active monitoring of uncommon activities in networks.

Improving the security of cyber infrastructure increases the costs that an attacker must incur to carry out a successful cyber-attack, and makes it less likely that the attack will have the desired effects and gains. If opponents know beforehand that the defense of a certain cyber infrastructure is well constructed, they will be less likely start a cyber-attack (but instead may look for other ways to attack – or attack another potential victim). To achieve this, the cyber infrastructure must be secured in such a way as to ensure that any attackers encounter barriers that considerably reduce the likelihood of their attack succeeding.

Cyber defense is regularly regarded as the best way to deal with international cyber threats.[5] An important problem, however, is that cyber defense is expensive and complex and requires continuous investment; technological developments occur at such a rapid rate in the cyber domain that any stagnation means decline. In addition, it is difficult to raise full awareness on the part of all people involved. Cyber-attackers always exploit the weakest link in the chain that they can find, and often, these weakest links are human beings. A cyber-attacker targeting a certain organization will need only one inattentive employee who downloads infected files, thereby creating an opening for the cyber-attacker.

Another problem with deterrence by denial is that cyber-attackers always have the advantage of time to look for weaknesses in cyber infrastructure, while the targeted party must respond as soon as a previously unknown weakness is exploited. In other words, cyber-attackers always have the element of surprise, making defense more complicated. Even more, because cyber-attackers immediately look for other weaknesses as soon as a gap in security has been closed, they always have an advantage over cyber defenders, especially because it is impossible to close every security gap in cyber infrastructure. Cyber defense will therefore always be a competition between attackers exploiting or seeking to exploit a newly discovered weakness, and defenders working to close a detected security gap as quickly as possible. From a deterrence perspective, cyber defense is only effective if it really changes the cost–benefit calculus of enemies. If the attackers consider it worthwhile to increase their efforts to surpass the improved cyber security measures, deterrence by denial has limited effect.

Deterrence by Retaliation

A more active method of deterrence is changing the cost-benefit calculus of potential cyber-attackers by openly communicating the possibility of retaliation and doing so if cyber-attacks are conducted. Retaliation of cyber-attacks could be done through retaliatory measures within the cyber domain itself (a cyber-attack on the attacker carried out by the party first attacked), diplomatic and/or economic sanctions, or even conventional military action. Furthermore, retaliation can be done overtly or covertly. To a certain extent, fear for retaliation will undoubtedly raise the threshold for cyber-attackers.

Economic retaliation of cyber-attacks through instituting (or strengthening pre-existing) economic sanctions might have some value as a deterrent, especially against countries with an economy that is highly dependent on trade relations with the retaliating state. However, once the sanctions are installed or strengthened, the sanctioned state has little reason to change its cyber behavior unless there are guidelines on how to ease or get rid of the sanctions. Another risk is that the economic interdependence is mutual, so economic sanctions will hurt the retaliating state as well. This is even more the case if the retaliated state will reply with counter-sanctions; in that case one could question whether the economic damage would outweigh the deterrent effect regarding cyber-attacks.

Retaliation by counter-attacks in cyberspace may be a more effective deterrent; the most obvious option to retaliate is to strike back in the same realm as the offender. The threat of counter-attacks in the cyber domain may considerably change the cost-benefit analysis of potential cyber-aggressors. On the other hand, retaliating a cyber-attack with another cyber-attack bears the risk of escalation through a tit-for-that cycle of cyber-attacks from both sides.

Another (though less realistic) option is retaliation through conventional military means, such as a strike against a specific location related to the cyber forces of the attacking state. Such an action may easily trigger a military response from the target state and could culminate in a dangerous process of escalation. This method seems likely to be considered only in the case of very destructive cyber-attacks, or if the attacker involved is considerably less powerful and will not be able to strike back militarily.

A final option of deterrence by retaliation is the use of covert military operations. It is the invisibility, and therefore unpredictability, of covert retaliation that might deter opponents from conducting cyber-attacks. Ideally, the opponent never knows whether arising cyber problems are created by covert retaliatory activities or other causes. Of course, covert retaliation also brings a risk of escalation: the target state may retaliate itself, and maybe for problems that were not caused by covert operations in the first place.

Even apart from the risk of escalation, various specific characteristics of the cyber domain make it relatively difficult to apply deterrence by retaliation effectively. The main obstacle is the attribution problem.[6] It is very difficult to conclusively identify the actor(s) responsible for unclaimed cyber-attacks. Cyber weapons differ from other weapons, as the origins of cyber weapons are not clearly visible and traceable. For example, attackers can use a chain of hacked or infected computers without the owners of these computers actually being aware of any wrongdoing. Although it is technically possible to locate the source of a cyber-attack by means of IP addresses, there is always the possibility that the source identified was merely a link in the chain of the attack and that the owner was not in any way deliberately involved in the attack.

In addition, state actors can conceal their involvement by having cyber-attacks carried out by non-state actors, like criminal hacker groups. Conversely, non-state attackers may claim an association with a given state even if this is not actually the case. It is even possible to plant "false flags" into cyber attacks, by deliberately leaving traces to another, non-involved actor (for example, by using language or computer codes linking this third actor). Because it is difficult to establish the identity of the actor responsible for a cyber-attack with absolute certainty, especially if the accused actor denies involvement, there is a risk of retaliating against an innocent party. In practice, few state actors will be willing to take this risk, something that cyber-attackers are well aware of. Strong forensic capabilities in the cyber domain are crucial to identifying the cyber-attackers; a higher probability of being identified will certainly have a deterrent effect. Currently, only very few states that have the capabilities to combine sophisticated cyber forensics with outstanding traditional intelligence operations may be able to acquire accurate, convincing evidence about cyber-attackers. Yet, openly presenting the evidence acquired may entail the risk of hurting future intelligence operations because opponents may gain insight into the intelligence capabilities that were applied.

The credibility of the retaliation threat and the risk of escalation are problems as well. Deterrence by retaliation only works if the party seeking to deter communicates clearly about the retaliatory measures that may be taken in the event of a cyber-attack. If communication about possible retaliatory measures is not clear, it is unlikely that a potential attacker will take them into account and they will therefore not have a deterrent effect. After all, deterrence measures are only effective if the opponent is aware of them. Moreover, drawing 'red lines' in the cyber domain can also have the opposite effect to potential opponents. Cyber-attackers may deliberately cross a red line to cause escalation, perhaps even while taking advantage of the attribution problem and posing as a different party. To maintain the credibility of deterrence, the party using it as an instrument must retaliate – even if doing so at that specific time is not the favored course of action. Any failure to adhere to the deterrence mechanisms communicated would dilute the deterrent effect, since potential opponents would be encouraged to think that the red lines are not all that red in practice.[7] From this perspective, deterrence by retaliation may increase the risk of a vicious cycle of escalating hostilities as well.

Deterrence by Signaling

A third category of cyber deterrence is actually a mix of deterrence by denial and deterrence by retaliation, which, on a scale of escalation risk, could be placed between the two. Deterrence by signaling is mainly about influencing the cost-benefit calculus of cyber-attackers through communication.

The foreign policy instrument of signaling consists of giving a signal to an adversary to express knowledge as well as discontent about certain behavior of this adversary. Thus, the actor in question may be convinced to stop the signaled behavior, realizing that any continuation will be noticed and potentially result in retaliation.[8] Generally, it is as simple as just communicating that the behavior of the adversary is known and deemed undesirable. This can be done in private, only known between the two adversaries, or in public, which makes the instrument more like "naming and shaming." Diplomatic protests (for example, expelling diplomats) or legal measures (for example, indicting specific persons involved with cyber aggression) are examples of mostly symbolic measures that have a signaling, and thus deterring, effect. Signaling aims to convince the adversary that continuing the activity in

To effectively deter cyber-attackers, their cost-benefit calculus needs to be influenced, leading them to conclude that the costs of launching a cyber-attack may be higher than the benefits.

question may result in countermeasures. This implies that effective signaling entails the (indirect) threat of potential retaliation as well. This way, the cost-benefit calculus behind the signaled behavior is influenced: continuing will be more costly than was (assumingly) expected before the signal was received. Yet, to support the signaling instrument, retaliation options must be on the table. Without the risk of being retaliated against, signaling efforts will less easily impress the cyber aggressor.

Although signaling is often done in private, between two influential officials or politicians, doing it in public may have even more of an effect. Public naming and shaming could have negative consequences for the adversary state's reputation, with potential repercussions in the political and economic realm. The attribution problem in the cyber domain and the risk of escalation should be mentioned here as well, but the negative effects are less direct than applying deterrence by retaliation immediately. When using the instrument of signaling, it may be less necessary to provide 100% convincing evidence as compared to retaliation.

Especially in the cyber domain, signaling may be an effective deterrent. Cyber weapons are generally considered as almost "cost free." They are often effective, while being relatively cheap to use. Moreover, because of attribution difficulties, the anonymity of the user is to some extent guaranteed. Signaling, however, could change this cost-benefit calculus. If applied successfully, signaling could remove the perceived anonymity of the cyber aggressor.[9] Signaling thus provides foreign policy makers with an extra escalation level, with only psychological effects, before the next level of actual retaliation.

Diplomacy as a long-term solution

An important notion when discussing deterrence in the cyber domain is that deterrence may be effective in the short term, but diplomacy is most promising to contribute to international cyber security and stability in the long term. While deterrence policies may almost directly have positive effects on a state's cyber security, they are expensive and bear the risk of continuing escalation. Diplomacy may not offer any "quick fixes" regarding cyber security problems, but in the long term it could offer a more secure and stable international environment in which cyber-attacks conducted or supported by state actors becomes less likely.

Confidence-building measures, for example, could enhance interstate cooperation, transparency, and predictability, with the aim to reduce the risks of misperception, escalation, and conflict entailed by cyber threats. In case of cyber aggression, confidence-building measures could function as pressure valves, allowing a safe release of tensions before they escalate. Also important are international norms and values established by multilateral diplomacy; they are to a large extent "invisible", but very influential to international security and stability. Globally-shared norms against the use of nuclear weapons, for example, contributed to the fact that their use has been nearly unthinkable for many decades. Diplomacy may contribute to establish similar norms regarding cyber-attacks. Norms can provide shared understandings between states, allowing them to consider shared interests, as well as finding ways to deal with diverging interests. Yet, the diplomatic route to establish international norms regarding cyber security is not a short-term process. To come to broadly accepted norms, common values have to be found; states must perceive that following the norms is in their own national interest.[10]

Conclusion

Deterring large cyber-attacks is not an easy task for states. To effectively deter cyber-attackers, their cost-benefit calculus needs to be influenced, leading them to conclude that the costs of launching a cyber-attack may be higher than the benefits.

Three categories of cyber deterrence policies have been discussed above: "Deterrence by Denial" mainly means investing in cyber defense measures. It does not involve much risk for escalation, but in its passiveness it may not convince cyber-attackers to stop searching for loopholes in the cyber defenses – which will definitely be found. "Deterrence by Retaliation" is a more aggressive method: it is about ensuring cyber-attackers that they will face serious consequences when their activities are discovered. This method may have more deterrent power, but also bears serious risks of escalation and ongoing (cyber) conflict. Last, but not least, "Deterrence by Signaling" was described as a policy option. This method, which is about communicating to (potential) cyber-attackers what is known about them and what will not be tolerated, fits in between the other two options on a scale of costs, risks, and effectiveness. Ideally, a state combines all three methods in a flexible mix of cyber deterrence methods. Yet, it is also preferable that states not only focus on short-term deterrence policies, but also invest in diplomatic efforts, which may be more effective in the long term.

Sico van der Meer is a Research Fellow at the Netherlands Institute of International Relations 'Clingendael'. His research is focusing on non-conventional weapons like Weapons of Mass Destruction and cyber weapons from a strategic policy perspective.

Toward a Global Norm Against Manipulating the Integrity of Financial Data[1]

Tim Maurer and Steven Nyikos
Carnegie Endowment for International Peace

In 2015, the heads of state of the world's twenty major economies agreed to specific language about rules of the road for cyberspace in their G20 summit outcome communiqué. The heads of states affirmed that international law - in particular, the UN Charter - is applicable to state conduct in the use of information communication technologies (ICTs), and declared that all states should abide by norms of responsible state behavior in the use of ICTs.[2] World leaders thereby explicitly endorsed what a group of governmental experts had developed under the auspices of the UN only a few months earlier. These UN groups of governmental experts (UNGGE) have been the main vehicle for the international community to discuss these issues ever since the Russian Federation put them on the agenda of the UN General Assembly's First Committee, which focuses on international peace and security, in the late 1990s.

The most recent development is the March 18, 2017 communiqué by the G20 finance ministers and central bank governors. They highlighted that:

> "The malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability. We will promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20. With the aim of enhancing our cross-border cooperation, we ask the FSB, as a first step, to perform a stock-taking of existing relevant released regulations and supervisory practices in our jurisdictions, as well as of existing international guidance, including to identify effective practices. The FSB should inform about the progress of this work by the Leaders Summit in July 2017 and deliver a stock-take report by October 2017."[3]

This statement is not surprising. The financial crisis that erupted in 2007 highlighted how fragile and important trust is for the global system. And the 2016 Bangladesh Central Bank cyber incident exposed the new threat to financial stability and the unprecedented scale of the risk that malicious cyber actors pose to financial institutions.[4] This invites the question: How do existing efforts to shape norms of state behavior in and throughout cyberspace relate to the global financial system?

Among the UNGGE reports, the most relevant is the 2015 report outlining a peacetime norm focusing on critical infrastructure, stating that:

> *Beyond theft, using cyber operations to corrupt the integrity of data, in particular, poses a distinct and greater set of contagion risks than other forms of financial coercion.*

> "[A] State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[5]

This UNGGE effort and the G20 statements are commendable, but still lack enforceable commitments or concrete steps toward a robust international regime.

Pursuing agreements with greater detail in expectations, rewards, and consequences is therefore a logical next step. We propose to focus on the global financial system: specifically, the integrity of data of financial institutions. This sector is uniquely interdependent on a global scale and highly reliant upon ICTs compared to other segmented infrastructure. The impact of an electrical grid cyber-attack, for instance, may be limited to one country or region. Meanwhile, the impact of the manipulation of financial data and erosion of trust can cascade worldwide and pose significant blowback risk. The financial system is therefore particularly desirable for world powers to protect.

Beyond theft, using cyber operations to corrupt the integrity of data, in particular, poses a distinct and greater set of contagion risks than other forms of financial coercion. The complex and interdependent character of the financial system and its transcendence of physical and national boundaries means that manipulating the integrity of data of financial institutions can, intentionally or unintentionally, threaten financial stability and the stability of the international system. Importantly, unlike the 2007/2008 global crisis, this risk exists independent of underlying economic fundamentals and will only increase as more and more governments make cashless economies an explicit goal.[6]

Major world powers have recognized these risks and demonstrated restraint. For example, the U.S. government refrained from attacking Saddam Hussein's financial system, and acted similarly in simulations of conflict with China.[7] Russia recognized this risk in its "Draft Convention on International Information Security," suggesting "each State Party will take the measures necessary to ensure that the activity of international information systems for the management of the flow of…finance… continues without interference."[8] China, in turn, has an interest in a stable system after advocating for the Renminbi to become part of the IMF global reserve currency basket. Meanwhile, India strengthened their financial sector Computer Emergency Response Team (CERT) as recently as February of 2017.[9]

The G20 heads of state could therefore adopt the following language at their next summit:

- *A State must not conduct or knowingly support any activity that intentionally corrupts the integrity of financial institutions' data (and algorithms) wherever they are stored.*

- *To the extent permitted by law, a State must respond promptly to appropriate requests by another State to mitigate activities corrupting the integrity of financial institutions' data (and algorithms) when such activities are passing through or emanating from its territory or perpetrated by its citizens.*

This approach has three key elements: states commit not to intentionally corrupt financial data, states agree to respond to requests for mitigation of financial sector attacks, and states' private sectors would be expected to follow due diligence standards and best practices. Linking national commitments with private sector obligations addresses moral hazard concerns, and an obligation to respond shifts the burden of attribution from the victim of attack to states that profess interest in helping to respond to and ultimately prevent such attacks.

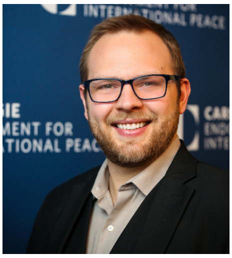
Such an agreement would send a clear signal of the importance of preserving the integrity of financial data in peacetime and war to the international community. Further, it builds confidence among states that already practice restraint, and thereby increases their leverage to mobilize the international community if the norm is violated. Additionally, the norm creates political momentum for greater collaboration to tackle non-state actors who target financial institutions with cyber-enabled means while complementing and enhancing the 2015 UNGGE report and 2016 CPMI-IOSCO *Cyber Guidance*.

Historical analogies and the international experience in outlawing counterfeiting currencies may be instructive here. States have adhered to and helped enforce the prohibition against counterfeiting because there is widespread mutual vulnerability to its effects. And because this restraint is widely accepted, states violating it are highly likely to face punishment. Non-state actors, of course, persist in counterfeiting, as do North Korea and a few other states, but the practice is contained enough that it does not threaten the stability of the international financial system.[10]

Another historical analogy conveys why major economic powers such as the G20, at least, would have interests in endorsing and upholding a specific norm against manipulating financial data in peacetime and in wartime: the British government using its dominant position in the global trade and financial system in 1914 to conduct economic warfare against Germany. The strategy succeeded at deranging the German economy, but after only three months the British government abandoned it. The backlash occurred far more intensely and faster than anticipated, including protests from UK businesses, laborers, and political figures, and pressure from allies.[11] The then-highly integrated nature of the global economy made it impossible to contain the blowback from an economic attack.

Ultimately, such an agreement would make explicit what could be considered the emerging state practice to refrain from manipulating the integrity of data of financial institutions. Of course, in the twenty-first century, a few states that are relatively detached from the global economy - and non-state actors who may or may not be affiliated with them - could conduct cyber-attacks against financial institutions. Yet, the states that did explicitly endorse such a norm would be more united and would have a clearer interest and basis for demanding an end and potential retaliatory action against violators of the norm, be they states, terrorists, or cybercriminals. The G20 could powerfully advance this norm by articulating it when they meet next, building on the mid-March finance ministers' statement.

Tim Maurer is a fellow at the Carnegie Endowment for International Peace and co-directs the Cyber Policy Initiative. His research focuses on cyberspace and international affairs, namely cybersecurity, human rights online, and Internet governance.



Steven Nyikos is a research analyst with the Cyber Policy Initiative at the Carnegie Endowment for International Peace. He focuses on digital sovereignty and ICT supply chain integrity.

Beyond Ones and Zeroes: reframing cyber conflict

Miguel Alberto Gomez
Center for Security Studies (ETHZ)

Introduction

Over the past decade, a steady stream of cyber operations has captured the imagination and stoked fears of the public at large. The possibility that a society increasingly reliant on cyberspace is at the mercy of actors capable of exploiting this dependency has been parroted across different quarters – from politicians, military leaders, and even academics. Since the worrying events in Estonia in May 2007, state-associated actions in cyberspace have grown increasingly complex – and with it our assumption of its strategic potential. Yet, interestingly, despite advances in their capabilities and increasing reach, most attacks have been viewed as strategically insignificant. The Distributed Denial-of-Service (DDoS) attacks against Estonian infrastructure, for instance, achieved little in coercing the Estonian authorities to shift their policies in favor of Russian interests. Similarly, the attributes associated with Stuxnet in 2010, despite being the first instance of physical damage resulting from cyber operations, did not dramatically hinder the Iranian nuclear programme. Ironically, it may have instead hardened Iranian resolve and jumpstarted their own cyber warfare program (Iasiello, 2013).

Inversely, lesser-known operations characterized by reduced sophistication and dramatic effect have resulted in noticeable gains. The BoxingRumble operation, part of the Snowden disclosures, demonstrated how the United States government had managed to discourage further Chinese espionage attempts against NIPRNET. Similarly, the OPM Hack did not result in any physical damage, but led to high-level talks between the American and Chinese governments to establish proper behavior in cyberspace (Jensen et al., 2016). With these interactions and their outcomes in mind, what are we to make of the state use of cyberspace? Is its strategic utility as espoused by its proponents during the first few years of the 21st century simply overrated? Perhaps not. While most of these events have not met their stated objectives, or at best have been tactical rather than strategic wins, one cannot discount their potential utility (Healey, 2016).

In so doing, this essay argues that perhaps the time has come to reorient our views with respect to the nature of cyber conflict. This essay proposes that two shifts are necessary before one can dismiss the strategic utility of cyber operations. First, we must begin to prioritize strategic considerations over technological determinism. The case of cyberspace heralding a revolution in interstate relations (e.g., war) is neither the first nor the last instance of technological enthusiasm. Similar sentiments were shared with the advent of airpower only to be firmly restrained through its continued use. Second, the notion of success in cyberspace must be framed in the context of heterogeneous threat perceptions. While there is no discounting the fact that cyberspace continues to make significant inroads across

... perhaps the time has come to reorient our views with respect to the nature of cyber conflict.

different societies and states, its valuation is by no means uniform. A cursory review of policy documents across states highlights different conceptualizations of cyberspace (Shafqat & Masood, 2016; Luiijf et al., 2013). This incongruity results in contrasting threat perceptions that, in turn, affect what one state would view as either victory or defeat. Borrowing from Wendt, it can thus be said that cyberspace is what states make of it.

Beyond Technology

The earliest discourse surrounding the strategic utility of cyber operations focused on the unique technological characteristics of the domain. Noting the "low cost of entry," difficulty with defense, and attributional challenges, proponents of what has been termed as the "cyber revolution thesis" believe that previous strategic thought does not and ought not to apply (Liff 2012). Given the rapid rise in the adoption of Information Communication Technologies (ICT) from the mid-1990s onward, one cannot be blamed for finding merit with this argument. Unfortunately, the historical record lends limited empirical support to such an astrategic view of cyberspace.

To begin with, most state-to-state exchanges in cyberspace have involved rivals. Maness & Valeriano have demonstrated that operations involving actors with enduring rivalries have nearly quadrupled since the year 2000. Moreover, issues such as territorial disputes and regime legitimacy have framed these interactions. It is of note that several of these actors have exercised a degree of restraint in cyberspace (Maness & Valeriano, 2015b; Maness & Valeriano, 2015a; Valeriano & Maness, 2013). Despite the notion that it is a relatively cheap domain to enter, these interactions are dominated by states with notable economic and military capabilities (Pytlak & Mitchell, 2016). Given the limited number of actors coupled with investment costs associated with cyberspace, the initial assumptions surrounding the domain are increasingly challenged. Yet, what about the question of defense? If highly capable actors are indeed utilizing cyberspace, shouldn't its use be maximized? To this end, it has been argued that the fear of escalation may be restraining overly aggressive behavior (Lawson, 2013). Despite the uncertainty in attribution, the small pool of participants involved and the issues surrounding most of these events minimizes the fog of uncertainty. So much so, that leaders like former US President Barack Obama have noted the possibility of a kinetic response to attacks in cyberspace.

Thus, the notion that cyber operations exist beyond the bounds of strategy is unfounded. As noted by Colin Gray, "cyber power is the ability to do something strategically useful in cyberspace" (Gray 2013). Yet, this requires one to establish a link between strategic interests and cyberspace. Unlike concerns surrounding the utility of cyber operations, this is far less contentious. Kuehl and succeeding scholars agree that cyberspace serves as an enabler for several instruments of national power that, in turn, serve strategic interests. Objectives including economic growth and military efficiency have been enabled by rapid developments in the domain (Kuehl, 2009; Starr, 2009; Nye, 2010). Consequently, the ability to employ cyberspace to further these objectives while hindering those of a rival's determines the expected utility of cyber operations.

And, yet, a caveat exists. States do not have a standardized view of cyberspace (Giles & Hagestad, 2013). This implies that the level of support that cyberspace offers to specific instruments is inconsistent across states. For instance, while the United States may be able to alter the operations of critical infrastructure in China, this is far less worrying to the existing regime than if their adversary were to launch an information campaign through Iranian cyberspace. This view is strengthened if one were to observe that China's priorities seem to lie in censorship and content management rather than the overall security of their infrastructure (Lindsay, 2015). Ultimately, the expected utility of cyber operations is inherently linked to varying threat perceptions that emerge from differing conceptualizations of cyberspace.

Victory and Threat Perception

The question as to the exact nature of cyberspace continues to persist in this nascent field. Despite the unlikely appearance of consensus, cyberspace can be divided into two different conceptualizations. The first treats the domain as a technology-dependent space. This includes both the technology and the information flowing through it. Adherents of this view – also referred to as the "western consensus" – see in it an enabler of economic and political processes. Furthermore, this perspective is shared by states with liberal regimes that see in it a platform for spreading liberal-democratic values. In contrast, the second treats the domain as the space between technology where information exists. This encompasses the mind of individual users that participate in cyberspace. While this treatment also treats the domain as an enabler, it goes further by bestowing upon it societal and ideological value. Illiberal regimes, fearing the possibility of a counter-narrative from cyberspace challenging their legitimacy, often view cyberspace in this light (Rivera, 2015; Hare, 2012).

These two views, inclusive and exclusive, result in different prioritizations that influence threat perception. Most existing research into the utility of cyber operations fail to take this into account. This leads to the propagation of the belief of the astrategic nature of cyberspace (Gray, 2013). To demonstrate this point, the case of Stuxnet proves instructive. From the American perspective, their inclusive treatment of cyberspace could, in some sense, lead to the idea that Stuxnet was a victory (tactically). Since value is placed on the ability of cyberspace to support strategic interests (i.e. targeting Iranian centrifuges through cyberspace) would hinder their strategic goal of enriching Uranium. This logic is seen in other cases such as BoxingRumble wherein the disruption of the espionage network hindered the strategic objective of obtaining information.

On the Iranian side, however, a different mechanism is seen. While damage was inflicted on their equipment (albeit minimal), the lack of a significant response from the regime suggests that their valuation of cyberspace as a key enabler of their strategic interests vis-a-vis their nuclear program was weak. Although it may be argued that the limited damage could in part have mitigated a more vociferous response, their behavior in other instances is telling of their priorities in this domain. While the idea that Iran tightly censors the Internet is correct, this has not always been the case. During the initial years of its introduction, the regime had been quite liberal relative to the region in allowing its citizens to use it as a platform for interaction and exchange. It was not until the appearance of rhetoric deemed subversive to the interests of the regime that steps were taken to regulate this space (Rahimi, 2003; Deibert & Rohozinski, 2010). It can then be argued that Iran perceives threats emanating from content rather than availability as a higher priority. In this respect, the Stuxnet operation was not viewed as a success on the part of the Iranians.

A Return to Strategy

Given the previously raised points, it would be foolish to haphazardly dismiss the strategic utility of cyber operations. While the historical record does not appear to adhere to the aspirations of its proponents, the utilization of cyberspace is by no means futile. Instead, special consideration ought to be made for how it is employed and its outcomes interpreted. First, one must acknowledge that cyber operations do not exist outside the bounds of strategy. Airpower, despite the notion that it would render rival state helpless and force them to one's will, had much less influence than originally proposed. Its critics have argued that context mattered in its exercises. Second, while it is indeed correct to suggest that the increasing ubiquity of cyberspace may render states more vulnerable, it does not do so consistently. Threat perception varies to the extent that, where one might view danger, another might deem it insignificant.

With the trend in state use of cyber operations showing no sign of abating, it becomes even more important to keep these points in mind. Promoting the view that cyber operations exist beyond strategy encourages its reckless use that could promote further instability in the international system. In contrast, understanding that it forms part of a state's toolbox that is to be applied carefully and at the proper time may lead to the emergence of behavioral norms that could stabilize this increasingly important domain.

Miguel Alberto Gomez is a senior researcher at the Center for Security Studies. He holds a Masters degree in International Security from the Institut Barcelona d'Estudis Internacionals. He has previously worked as a lecturer at both the De La Salle University and the College of St. Benilde in the Philippines and has worked in the Information Security industry for the past eight years. His area of research is centered around Cybersecurity. Specifically, he is interested in the strategic use of cyberspace as an instrument of national power as well the emergence of norms surrounding the use of this domain.

Deciphering the “Hacking Back” Debate: questions of propriety and risk

Tim Ridout
German Marshall Fund

Currently on the agenda of the U.S. Congress are efforts to allow private entities greater leeway to protect their interests in cyberspace. The long-simmering debate is partly manifested in the form of a draft bill presented for discussion in February 2017 by Representative Tom Graves, a Republican of Georgia. The conversation raised by the draft bill is an important one, drawing on a great deal of work already done by leaders in the Washington debate on the matter, including a major analysis on active defense measures published by the George Washington University Center for Cyber and Homeland Security. Though the multi-institution authors did not reach a consensus on recommendations, the discussion is useful to read in its entirety for anyone seeking to understand the contours of the debate. It also comes at a time when an international commission has recently been formed by some major leading voices in the international debate, known as the Global Commission on the Stability of Cyberspace.

International lawyers, security experts, law enforcement officials, and others are already opining on the draft bill, both in terms of its wording, and whether or not it is a good idea. Robert Chesney, a legal scholar at University of Texas School of Law, recently offered a series of questions and comments on the Lawfare Blog at the Brookings Institution, which elicited a response from Herb Lin, a scientist and policy expert on cyberspace and cybersecurity at Stanford University’s Hoover Institution. Graves himself held a panel along with Representative Kyrsten Sinema, a Democrat from Arizona, and leading experts on May 1 at Georgia Tech. Listing everyone who commented on the debate would be impossible, but it suffices to say that Rep. Graves has been successful in his goal of at least starting a serious conversation on updating the Computer Fraud and Abuse Act (CFAA) with regards to the set of questions commonly referred to as “hacking back.” The issues are refreshingly bipartisan at a time of deep division. There are fault lines in the debate, but they are less about partisan affiliation and more about risk tolerance, propriety, and feasibility. With these concerns in mind, starting with a licensing process might be the best approach.

The proposal carries inherent risks if private entities are “deputized” under U.S. law to engage in what could be called “self-help” in the event of ongoing intellectual property theft, ransomware attacks, and other forms of continued harassment in cyberspace. The draft bill would allow victims of “persistent unauthorized intrusion” into their computers to essentially respond by intruding back into the originating computers to halt the intrusions or gather evidence to share with law enforcement. Such actions would otherwise be illegal for a private entity under CFAA. There is a seemingly intuitive logic in being able to defend one’s own interests, but carelessly penetrating someone else’s computer systems – especially in a foreign country - could open both the private sector actor and the United States government to significant liability and risk. If private entities make a mistake while operating with authority under U.S. law, the federal government may be drawn into an international incident, particularly if innocent third parties are accidentally harmed. Moreover, it could signal to the rest of the world that such activities are acceptable, and encourage foreign actors to reciprocate against U.S. companies and other private entities. Of course, the counterargument is that this activity already occurs daily, and these private entities would merely be responding in kind.

> Allowing private entities to unilaterally decide when to penetrate someone else's networks is probably too risky and would open up new forms of unforeseen liability.

But, what if the "hacktivist collective" known as Anonymous - or a similar group - decided that they were now legally permitted to operate within U.S. territory to target entities that they believed to be fair game? Such groups, often acting out of a sense of moral outrage and believing their cause to be just, might not understand the local cultural and legal context. This could mean that they accidentally harm those they seek to help or place a burden on U.S. authorities due to the international norm that states should do their best to ensure that malicious non-state cyber actors do not use their territory. Moreover, it may be difficult to verify compliance under the CFAA if the door is opened to self-help, and it could lead to a heavier workload for law enforcement if they have to police newly emboldened cyber vigilantes. These risks do not seem well understood.

The ideas behind the proposed legislation could be viewed as a way to increase the overall capacity of the U.S. private sector to support the work done by the FBI and other agencies, but whether or not that would come to pass is anyone's guess at this point. A more cautious first step might involve a licensing process. Rather than generally permitting anyone to interpret "persistent unauthorized intrusion" as they see fit and take matters into their own hands, authorizing certain large entities such as financial institutions, energy companies, and utility operators to hack back through a rigorous and regularly renewed licensing process could be a way to experiment with innovative approaches without going overboard. Specifying that only highly sophisticated, previously vetted entities are lawfully permitted to penetrate an aggressor's systems for the sake of gathering evidence or halting ongoing intrusions could enable a tougher approach while minimizing new risks. Indeed, I would think it would be necessary to assign strict fiduciary responsibility and legal liability to any person or entity engaging in hacking back under CFAA if the legislation does become law, with regular reviews of their activity and periodic required training in order to renew what could be considered a "license to hack back." Allowing private entities to unilaterally decide when to penetrate someone else's networks is probably too risky and would open up new forms of unforeseen liability.

The decision about whether these are good ideas as matters of policy is ultimately for the U.S. Congress and Executive Branch to make, but the wording of the draft bill clearly requires modifications to ensure that the intent of the legislation is captured in carefully circumscribed legalese that leaves no room for vigilantism in cyberspace.

This draft legislation should also be seen in the context of the international community's growing efforts to make cyberspace more stable and secure, especially since nation-states seem to be formally weighing in on some of these debates more often, as discussed by leading experts Jason Healey and Tim Maurer in a recent article in CSM Passcode. It might not be worth it if the bill is seen as contrary and unhelpful to those efforts by encouraging destabilizing unilateralism in an already anarchic international cyberspace environment - even if it seems to make sense when viewed in isolation. Maintaining multilateral cooperation and managing international relationships are critical to addressing these challenges, meaning that drastic changes in approach should at least be done in consultation with friends and allies.

Whatever the specifics, there is a general consensus in the United States and many other countries that something needs to change in how we approach stability and security in cyberspace. It will not be a one-off fix, but rather an ongoing effort by governments, citizens, and stakeholders around the world to make our networked world work better for more people.

Tim Ridout is a non-resident fellow at the German Marshall Fund of the United States (GMF), where he focuses on political and economic issues in Brazil, in addition to U.S. foreign policy and cyber strategy. Prior to joining GMF, he worked at Institutional Shareholder Services as a corporate governance analyst, primarily studying Brazilian companies. Before that, he was a program manager with the Brazil-U.S. Business Council at the U.S. Chamber of Commerce. He spent his early career working at law firms focused on litigation, health care, and corporate strategy.

Cyber Security Related Behaviors, Data Privacy, and Challenges Ahead

Interview with Professor Jason Hong
Carnegie Mellon University

Much of your research has centered on the intersection of computer and behavioral science. Would you share some highlights of that work?

How can we get people to change their cyber security-related behaviors? How can we improve people's awareness, knowledge, and motivation to be secure online? One of our research thrusts is called Social Cybersecurity, which looks at how to use social influences to change people's behaviors. For example, in one study we did with Facebook, we added messages to people's News Feed, telling them things like "108 of your friends use extra security settings, click here to learn more" or "10% of your friends use extra security settings, click here to learn more." These messages leveraged the idea of social proof, helping people understand what others are doing. Past work in social psychology suggests that simple messages like these should change people's behaviors, and our experiment confirmed it. We found that many more people clicked on these messages and adopted some of the extra security settings than those who just received a message mentioning extra security settings.

Another line of work our team has looked at is understanding what personal data your smartphone apps are actually using. Many apps have unusual behaviors. We've found a Blackjack app that uses your location data, a motorcycle racing app that uses the microphone, and a Bible app that uses your contact list. We built PrivacyGrade.org to surface these kinds of unusual app behaviors, assigning grades to each of the million-plus apps that exist on Google Play. We developed a simple computational model of privacy based on people's expectations of privacy. For example, most people don't expect a motorcycle app to use microphone, so if it does, then we consider this a big privacy problem. In contrast, almost everyone is aware that Google Maps uses location data, so we don't consider that to be a privacy problem.

What best practices should developers adopt to improve cyber security in applications?

One of the big challenges for cyber security today is that most developers don't have much experience with secure programming. About half of developers today have a computer science degree, and even then, only a handful of the top 50 university programs require students to take a course in security.

Having said that, there are some pretty easy things that developers can do. For example, don't use common and well-known default passwords for devices, turn off network ports that aren't

> *One of the big challenges for cyber security today is that most developers don't have much experience with secure programming.*

being used on a device, sanitize user input to avoid SQL (Structure Query Language) injection and buffer overflow attacks, and use encryption when sending data over the network.

The challenge is that there are a lot of these easy things, and it can be difficult for developers to find all security-related bugs. Instead of suggesting specific features, I would instead recommend that developers have a better process for developing software. More specifically, I would recommend that developers look up checklists for secure programming (there are lots of these online), use existing tools to look for common and well-known classes of vulnerabilities (there are also lots of these available, both for free and for pay), and do periodic code reviews to look for bugs.

Data privacy is a growing concern for many, particularly as ubiquitous computing expands. In your opinion, how prevalent are serious data privacy issues? What would you prescribe to quell any unwarranted or inflated fears about data privacy?

Privacy is perhaps the greatest barrier to a connected world. There are numerous research papers, books, op-ed pieces, and news articles expressing people's deep concerns about what data is being collected about them and how it is being used. A lot of people might point to Google and Facebook and say that people don't seem to care, that privacy is dead. I think it's more nuanced than that — people's conceptions of privacy are changing. It's also worth pointing out that people react very negatively when they discover nasty surprises about how their data is being used. When I give presentations about my research investigating smartphone apps, I've had many people come up to me afterward saying that they deleted apps off of their smartphone because they were so shocked to learn what their apps were doing.

In the long-term, I think this is not a good thing, because we ultimately lose the value of having fun and useful apps. If we can figure out how to legitimately address people's privacy concerns, then we could make things into more of a win-win situation for all parties.

There are lots of possible approaches here, ranging from having intelligent privacy assistants, to helping developers develop privacy sensitive apps, to better models of people's decision making processes. One angle of attack that I'm especially interested in is addressing the market failure for privacy. Basically, if you go to a store and buy a networked gadget, it's easy to see if the device is aesthetically pleasing, and you can also read reviews or see other people using it to get a sense as to whether it would be useful and usable for you. In contrast, it's really hard to know what the privacy implications are. It's not something that's very obvious to consumers. It's also not a clear differentiable feature either, leading to developers neglecting the issue. This is a pretty clear market failure. Sites like PrivacyGrade.org help with smartphone apps, but we still need to figure out better ways of analyzing apps and expanding these analyses to the emerging Internet of Things.

Do you believe there are any significant cyber security issues that should be addressed by policy-makers?

There are a large host of specific issues that need to be addressed. One is more education and training at all levels, including K-12 and the workforce. Another is better coordination within and across organizations. For example, just in the United States alone, cyber security is split between elements of the Department of Homeland Security, Cyber Command, NSA, FBI, and more. It can be confusing to outsiders (and even insiders!) as to who is responsible for what. There's also the recent challenges of fake news, which makes it harder for democratic countries to have an informed citizenry.

From a broader perspective, what policy makers need to figure out are what are the right levers that can be used to address these and other problems. Cyber security requires diplomatic, economic, legal, as well as technical approaches, but right now our understanding of what works and what doesn't is still pretty primitive.

Moving forward, what do you envision as the biggest challenges for cyber security experts?

In the long-term, I think the biggest challenge for cyber security is Internet of Things. About 15 years ago, computers came in the form of large beige boxes that sat under our desk, along with a monitor, keyboard, and mouse. Today, a person can now go into any big box store and purchase smartphones, tablets, wearable fitness trackers, webcams, drones, smart thermostats, network-enabled toys, and more. Computation, communication, sensing, and actuation are being woven into the physical world.

However, these same technologies pose many new and daunting challenges for cyber security. Today, when attackers compromise your computer or your data, they might cause you financial harm, frustration, or embarrassment. Tomorrow, an attacker could lead to people dying. For example, what happens if an attacker compromises a self-driving car or an implanted medical device? There's also the issue of scale. We can barely manage the security of the laptops, corporate networks, and cloud infrastructure we have today. How can we protect the billions of smart toys, smart appliances, and smart buildings of tomorrow?

Jason Hong is Associate Professor at Carnegie-Mellon University, Human-Computer Interaction Institute. His research lies at the intersection of human-computer interaction, privacy and security, and systems. His research group is CHIMPS (Computer Human Interaction: Mobility Privacy Security), whose work has been featured in CNN, New York Times, BBC, CBS News, MIT Tech Review, World Economic Forum, and more.

Safeguarding Data Integrity in an Interconnected World

Edward M. Stroz
Stroz Friedberg, an Aon Company

Cybersecurity is one of the most consequential issues impacting organizations across industries and regions; and data theft, ransomware, privacy breaches, and other forms of cybercrime are on the rise. Attacks like these that target the confidentiality and availability of information tend to be high profile and highly visible, as they concern data privacy and access. However, no less pernicious but less visible is another significant concern: attacks on the integrity of data and the rising threat of data sabotage.

The important role that data plays in society requires that it be protected. Any social, economic or political organization that makes decisions or provides information based on facts is at risk of sabotage. Suppose an adversary hacked in to a city's systems for traffic lights on Election Day. As well as potentially causing traffic accidents, this would likely affect citizens' ability to arrive at the polls before closing. Accusations of voting fraud dominated the news cycle in the wake of the 2016 U.S. presidential election; a serious situation in a democratic society, and current proposed U.S. legislation addresses concerns about Russian interference in the 2017 European elections. Beyond the political sphere, imagine the damage that skilled attackers could cause if they compromised an amber alert system, or manipulated data to change the information that streams from a stadium screen during a big game, announcing a bomb threat. By making small changes in data, criminals have the ability to influence the behavior of large groups of people, causing panic, confusion, and undermining their ability to make decisions.

Healthcare is just one example of an industry that has evolved rapidly to become a data-intensive environment, which depends on the electronic exchange of patient information. Part of this evolution has included the rise of multiple platforms to capture, store, transform, transmit, and view data, and these devices and networks are increasingly interconnected. When data is manipulated, all resulting information organized based on those data facts is flawed. Looking at healthcare specifically, if data integrity is lost, an individual's blood test results entered into a database in March 2017 might appear substantially different when those results are reviewed in March 2019. Basing medical treatment and prescriptions on altered data could have devastating consequences for patients. Extend this level of

> If data loses its integrity, we stand to lose the common basis of fact.

data tampering to individual tax returns, business financial records, government jobs reports, graduate admission test scores, leaked political communications, or simply grades in a secondary school gradebook, and one can see the great risks inherent in loss of data integrity.

The broader cultural implications of living in a world in which confidence about what is factual has been undermined, and information sources lose our trust, are limitless. If data loses its integrity, we stand to lose the common basis of fact. The advent of fake news, and people reacting to false claims in the media as if they were real, is shining the spotlight on the powerful negative influence that attacks on information integrity can have. Organizations and individuals owe it to society to take the steps to foresee potential threats, certify data integrity is reasonably ensured, and provide people with a sound basis for believing integrity has not been compromised.

In an attack scenario, there are typically three qualities of information targeted: Attacks on confidentiality, integrity, or availability of the underlying data. Attacks on the availability of information are rapidly detected and designed to be noticed: the system is locked or goes down, and the victim must respond. Attacks on confidentiality are more difficult to detect. While it might take a hacker only eight days to breach a network, it typically takes six or more months to detect the incident. The most insidious attack is an attack on data integrity: the attack is largely silent, or invisible, and unless an organization is vigorously reviewing the accuracy of data, the victim might not even be aware that data manipulation has occurred. To secure data, we are called to protect data integrity with the same vigor and focus as we today protect data confidentiality. The new EU General Data Protection Regulation (GDPR), set to go into effect in May 2018, sets the bar in terms of giving attention to securing data confidentiality. Adhering to this regulation will require major adjustments to privacy programs for all EU-based companies, and companies that collect the data of EU citizens. Securing data integrity warrants the same level of thought, action, and protection.

Data integrity might be compromised for a variety of reasons, not all of which are criminal or intentional. For example, unintentional human error and transfer errors might result in data flaws, as might compromised hardware when a device or disk crashes. Alongside minimizing these types of unintentional errors, malicious causes of data integrity loss demand our attention. Organizations are at risk from the employee or other "insider" with access who deliberately tampers with data, and external adversaries who employ cunning techniques to corrupt data, including design and release of malware, hacking, and other cyber practices. Just as cyber criminals today deploy ransomware and demand bitcoin or cash payment, as in the case of Hollywood Presbyterian Hospital where staff members were locked out of computers and patient records were frozen, we are likely to see these same offenders exploiting data integrity attacks as an additional method of bringing distress upon victims. To combat this genuine threat, we need to take action before such an attack occurs, or what is sometimes called "getting to the left of 'boom.'" We need to think in terms of what can be done by our adversaries, not just what has been done up to now; this requires pre-emptive strategy and action, rather than solely investigatory responses.

This is a manageable endeavor, and proven data protection methods can be utilized to meet this challenge. The first protection principle is fundamental: create redundant back-ups of critical data and develop a golden master, or a time-stamped, physically segregated and protected copy of the data, which becomes the basis of truth. Golden master copies are hashed using established hash algorithms to calculate an integrity checksum, which can be used later to verify that the data has not changed. Crucial databases can be replicated and data quality checks conducted at set intervals. For example, all prescriptions written each day at a hospital are saved to a golden master, and a hash value is calculated. To manage the risk of internal employees editing data, organizations can ensure access levels are appropriate to responsibilities and position, as cybersecurity programs can be undermined by excessive access. Holistically speaking, an organization's overall cybersecurity posture can be strengthened by undertaking an assessment to evaluate cyber risks, conduct network and application vulnerability testing, and develop a resulting plan to improve defenses. Importantly, should data be compromised, organizations need a response plan in place to contain and mitigate damages, and rebuild trust.

Despite the widespread and destructive consequences of attacks on the confidentiality, availability, and integrity of data, cyber risk is one of the least understood risks for a large majority of organizations today. With the growing awareness of fake news and its influence on society, we may well be at a tipping point, with people recognizing that the news problem is just the tip of the iceberg. Once the integrity of some sources of data and information is lost, our ability to trust all data and information is eroded, which can lead to skepticism around what is being reported as the truth. Decision-making – whether in politics, business, or everyday life – becomes impossible if we lose the ability to discern between accurate and altered data.

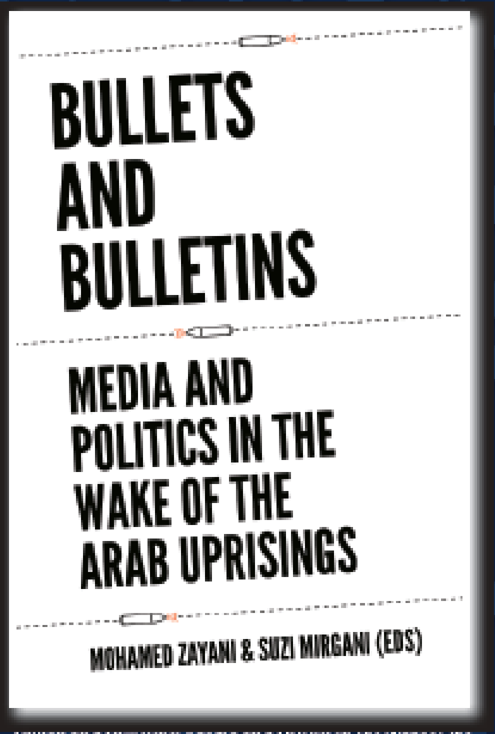
These risks should serve as an impetus for organizations to work towards becoming cyber resilient: the ability to prepare for, withstand, and recover from unanticipated incidents. Additionally, there is an obligation for thoughtful individuals, across regions and disciplines, to take the lead in envisioning what our adversaries can and might do – and to protect society against it.

Ed Stroz is the founder and Co-President of Stroz Friedberg, an Aon company and global leader in investigations, intelligence and risk management. Ed oversees the firm's growth and client development, while ensuring the maintenance of its distinctive culture. He also provides hands on strategic consulting in investigations, intelligence and due diligence, plus cyber and physical security. Before starting the firm, Ed was a Special Agent with the FBI where he formed their computer crime squad in New York. Trained as a Certified Public Accountant, he has extensive experience in investigations of white collar crime including bank fraud and securities fraud, and has testified in court numerous times as an expert witness. Ed is a trustee of Fordham University, his alma mater, and serves as an advisor to the Center on Law and Information Policy (CLIP) at Fordham Law School. Ed sits on the Board of Directors of the Crime Commission of New York City, an independent non-profit organization focused on criminal justice and public safety policies and practices, and is a member of the Association of Former Intelligence Officers. He also served on the New York State Courts System E-Discovery Working Group, established to provide ongoing support and expertise to the New York State Judiciary in the area of e-discovery.

جامعة جورجتاون قطر

GEORGETOWN UNIVERSITY QATAR

Center for International and Regional Studies

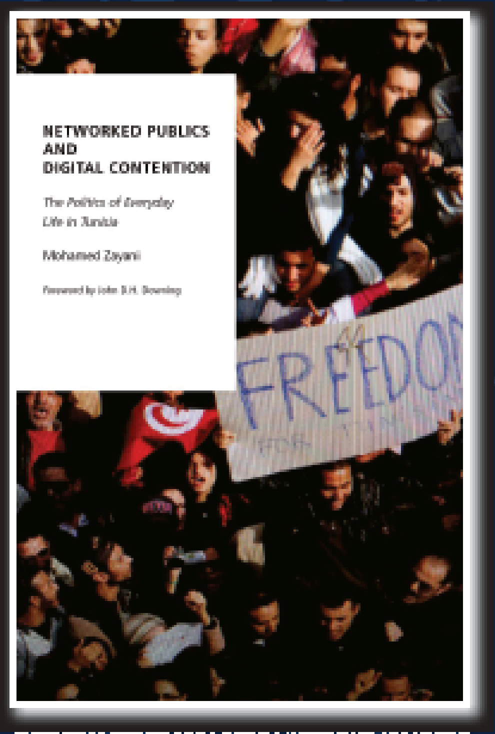


BULLETS AND BULLETINS

MEDIA AND POLITICS IN THE WAKE OF THE ARAB UPRISINGS

MOHAMED ZAYANI & SUZI MIRGANI (EDS)

Bullets and Bulletins: Media and Politics in the Wake of the Arab Uprisings, ed. Mohamed Zayani and Suzi Mirgani (Oxford University Press/Hurst, 2016), $35.00.



NETWORKED PUBLICS AND DIGITAL CONTENTION

The Politics of Everyday Life in Tunisia

Mohamed Zayani

Foreword by John D.H. Downing

Networked Publics and Digital Contention: The Politics of Everyday Life in Tunisia. Mohamed Zayani (Oxford University Press/Hurst, 2015), $27.95.

About CIRS

Established in 2005, the Center for International and Regional Studies (CIRS) at Georgetown University in Qatar is a premier research institute devoted to the academic study of regional and international issues through dialogue and exchange of ideas, research and scholarship, and engagement with scholars, opinion makers, practitioners, and activists.

Research Initiatives

CIRS engages in empirically-grounded, original research initiatives, and contributes towards furthering knowledge on issues related to information and communication technologies in the Persian Gulf and the broader Middle East. To download free publications, or to submit a paper, please visit: cirs.georgetown.edu/publications.

cirs.georgetown.edu

Machine Learning and Cyber Security

Interview with Anup Ghosh
Invincea, a Sophos company

Your company, prides itself as a next-generation computer security company. How would you define "next-generation computer security" and why is this significant for providing effective protection against cyber threats?

The model of anti-virus was defined in the 1990s based on the inoculation model from biology: given a sample virus, you could design a vaccine that immunizes a potential host or target. This methodology worked well for over a decade until computer malware attacks stopped looking like self-replicating viruses. Today's attack types are generated by exploit toolkits, which create an effectively infinite variety of malware, never re-using the same instance twice. An inoculation (signature) used to protect a machine from one variant of malware is often rendered useless from the next variant.

Next generation (next-gen) approaches must detect and stop the infinite varieties of malware otherwise known as previously unknown malware and zero-day exploits. Next-gen endpoint solutions employ machine learning, behavioural monitoring or isolation to detect and stop previously unknown attacks. Another key change in the adversarial landscape is the emergence of "file-less malware." These comprise attacks that do not drop a program on a disk, as a virus normally would. Instead, these attacks exploit system programs already on the machine for its own purposes such as Microsoft Office and Windows Powershell. Next-gen approaches must be able to identify and stop these file-less attacks that often include ransomware attacks.
Finally, traditional security architecture and solutions were often developed to address one particular type of attack as a point solution. Next-gen approaches bridge the gap between security sensors and controls throughout the enterprise architecture to not only share information between devices, but also synchronize their responses. An endpoint security solution that detects a previously unknown attack can directly share its knowledge and alert other devices, including those at the network perimeter, to stop those attacks from affecting other endpoints across the enterprise.

Explain your expertise: Machine Learning. How does machine learning play a part in "next-generation" cyber security and how does this impact businesses and end users right now?

Without question, most security solutions are now or soon will be adopting machine learning in the core of their offerings. The very attributes

Without question, most security solutions are now or soon will be adopting machine learning in the core of their offerings.

that make security hard for humans – extremely large volumes of data and effectively infinite permutations of code that derive from core malware DNA – make it a great fit for machine learning. Signature-based techniques are no longer effective against the sophisticated zero-day attacks we see today. Techniques such as deep learning neural networks can "learn" malware far better than humans. Each layer of a neural network learns features of malware, and when staged together, can identify previously unseen malware variants with high precision.

Businesses that are being compromised by unknown malware, zero-day exploits, spear phishing attacks, and ransomware attacks are discovering that next-gen approaches are very effective at stopping these attacks. Like any technology, good security technology is invisible to users, silently protecting the enterprise while enabling employees to use their devices in ways they want – browsing, social media and personal email - without fear of being compromised.

How does machine learning play a part in the future of cyber security? How will this technology evolve as will, most certainly, the threats themselves?

Machine learning is an apex technology in IT and software powering 21st century businesses. Security is no exception, and businesses that leverage machine learning-based security will keep pace with 21st century threats. Those that don't will fall behind if they have not already. Marc Andreeson noted, "software is eating the world." Well, machine learning is eating security. Ultimately, machine learning will replace a very human-intensive and unscalable security business model, with one based on data science and driven by very large data sets with algorithms curated by data scientists. While machine-learning algorithms have been around for decades, it is the convergence of cloud elastic architectures, big data science, and the commoditization of machine learning techniques for consumer applications, which is now driving this approach to power security applications.

Are there any threats in particular that Machine Learning is better at thwarting/ preventing?

While machine learning can be very effective at detecting variants of malware it is not a silver bullet solution to all threats and risks. Machine learning is often only as good as the data a model is trained with and the quality of the research in developing the algorithms. Completely novel attack types will tend to defeat machine-learning algorithms that only train on known malware.

A major threat that you work to prevent is spear-phishing. How so?

Spear phishing is perhaps the most vexing of all security attacks because it leverages human weakness to succeed. A good spear phish triggers an emotional response to get its target to open an attachment or click on a link. Security professionals depend on users to make the right decision every time a user opens an email – to click on legitimate links and attachments and recognize the malicious ones.

With isolation or "sandboxing" technology, you no longer have to depend on user's decisions to click or not. Anytime a user opens an email attachment or clicks a link, the attachment is opened in a virtual sandbox, which isolates the content from the rest of the system while monitoring it. If the content is malicious, it is killed and collected for threat intelligence.

What can everyday users do to better safeguard their internet usage? Phone usage?

First we must apply our natural suspicions of the physical world to the virtual world. If something sounds too good to be true, it probably is. In fact, we have less context for assessing the legitimacy of messages in the virtual world and must instinctively trust nothing until we have established that it is legitimate. Treat every unsolicited email with caution. Get the basics right, do: use two factor authentication or two step verification on important accounts, enable auto-updating on operating system, application and security software; don't: connect to unknown access points, plug in your phone to public charging ports, click on emails to login to your bank account, download unknown apps to your mobile devices, click on executable attachments or zip files, or wire money to save Nigerian princes. Practicing these basics on a regular basis will significantly reduce the risk of becoming a victim.

How large an issue is ransomware?

Ransomware is a type of destructive malware that is rapidly gaining traction. Based on what we expect, payments for ransomware could cross the billion-dollar threshold in 2017. The growth in ransomware payments will drive ever more ransomware campaigns, so don't expect to see this tail off anytime soon. We recommend that every business employ a security strategy that includes an anti-ransomware component, , to protect your data and device from being held hostage for a ransom.

DARPA recently held a hacking contest, challenging security bots (Cyber Reasoning Systems) to patch holes on their own. Do you see this as an effective path toward securing government systems from vulnerabilities?

DARPA grand challenges are a very effective way of spurring innovation from all sectors – large and small, academic and private, domestic and international. Often DARPA does this to prove the art of the possible. In this case, the challenge proved a machine can self-heal in the face of a changing adversary – an AI on AI type battle -- one AI to attack, the other to continuously morph and defend. There often is not a direct path to Government from these challenges. Ultimately, the technology if proven will make its way to the market via products and the Government will buy it for its IT infrastructure. A good example of this is the DARPA Autonomous Vehicle Grand Challenges of 2005 and 2006. The grand challenges resulted in ground breaking innovation that ultimately made its way into Google self-driving cars as well as influencing other auto manufacturers. DARPA's continued investment in security will be a catalyst for innovation throughout the industry.

Anup Ghosh is Chief Strategist, Next Gen Endpoint at Sophos. Ghosh was previously Founder and CEO at Invincea until Invincea was acquired by Sophos in March 2017. Prior to founding Invincea, he was a Program Manager at the Defense Advanced Research Projects Agency (DARPA) where he created and managed an extensive portfolio of cyber security programs.

He has previously held roles as Chief Scientist in the Center for Secure Information Systems at George Mason University and as Vice President of Research at Cigital, Inc. Anup has published more than 40 peer-reviewed articles in cyber security journals.

He is a frequent on-air contributor to CNN, CNBC, NPR, ABC World News, and Bloomberg TV. A number of major media outlets carry his commentaries on cyber security issues including the Wall Street Journal, New York Times, Forbes, Associated Press, FoxNews, CSM Passcode, Federal Times, Market Watch and USA Today.

He has served as a member of the Air Force Scientific Advisory Board and the Naval Studies Board, informing the future of American cyber-defenses.

Cyber Risk and Cyber Policies

Interview with Nadiya Kostyuk
University of Michigan

What are the greatest domestic challenges facing nations attempting to bolster their cyber security efforts?

These challenges are unique to each country, but generally I'd name two challenges: 1) lack of resources, and 2) lack of cooperation between various actors (especially between private and public sectors). Recent years have seen an increasing number of attempts to deal with cyber security issues domestically. Countries often lack resources to face this new challenge, and many of their efforts are still in a nascent stage.

Due to the intertwined nature of cyberspace, efforts by individual nations and actors are no longer sufficient. A multilateral approach that entails closer cooperation between governments, public and private sectors, civil society groups, and others, can boost everyone's security in the online environment. Building cybersecurity capacity in Ukraine is one such example. As a result of the 2013 Target attacks, NATO countries decided to help Ukraine build its domestic apparatus to deal with its own cybercriminals. As a result, they provided resources and training to create the cyber police in the country. This demonstrates how beneficial cooperation (and resource-sharing) is for both parties.

Through your work with the EastWest Institute and observations you have made, can you elaborate on whether or not you believe that the international community can work together effectively to counter cyber threats?

EWI does excellent work using Track-2 diplomacy to build the bridge between international players who often have different approaches to cyber security. Communication and trust building between these players is the first step to success. Because of efforts like this, the international community can work together effectively to counter cyber threats. But, such work should start on a bilateral or regional scale, based around the issues that the actors have a common interest in.

How can states work with international and regional organizations to coordinate their cyber security efforts?

International and regional organizations can serve two purposes: First, they can serve as a forum and a mediator for international discussions, and second, they can provide guidance to the states on how to improve their cybersecurity measures. The 2004 Budapest Convention on Cybercrime is one such an example, creating an international treaty to address cybercrime by establishing a collaborative amongst nations. It has been recognized by over fifty states, making it the first significant step in improving cybersecurity.

Are there opportunities for states to cooperate and collaborate in cyber security efforts? What are the steps world leaders can take to enact joint state efforts to prevent the proliferation of cyber warfare?

Having clear definitions is the first step. Even though significant progress has been made in

> ...wealthier nations should help those nations with fewer resources to prevent them from turning into cyber safe-havens.

this direction, leaders often tend to talk "at" each other instead of talking "to" each other because of differing technical definitions (e.g., information security versus cyber security). Collaboration is the key. Due to the intertwined nature of the internet, collaboration between all actors is important. Certain countries have been advocating for the "splinternet", while others argue that such an approach towards the Internet governance would diminish what the internet stands for. Thus, trying to find common grounds amongst states is an important step. Additionally, wealthier nations should help those nations with fewer resources to prevent them from turning into cyber safe-havens.

Much of your research focuses on the perception of cyber risk and state cyber policies. Can you define cyber risk and describe recent state practices to mitigate it?

There are various definitions of cyber risk, depending on what industry or player you are talking to. In my current project, I decided to focus on individuals and investigate how they define cyber risk. Based on that definition, the next step of my research studies how an individual's perception of such risk affects their evaluation of a state's cybersecurity policies. Since the study is not over yet, I am unable to share the results.

Since individuals are part of the solution, the state promotion of education and awareness of so-called "cyber hygiene" is quite an important step. During the last 5 years, countries worldwide have been actively implementing cyber hygiene curricula - whether for their government employees or for elementary schools.

How can cyber conflict affect the daily lives of individuals within the international community? Can cyber conflict threaten the power of governments?

Cyber attacks have been actively used during the conflict in Ukraine. To give one example, an electric power grid was attacked twice, in both 2015 and 2016, which left people without power for several hours. This instance was defined as the first example of cyber warfare.

Furthermore, the website of the Ukrainian electoral commission was hacked during the 2014 Presidential election. In 2016, the United States experienced the Democratic National Committee (DNC) hack.

It is important to understand that, even though the first-order effects of cyber-attacks might be minor, the second-order (long-term) effects are not always predictable and can be quite devastating.

In many European states, cybercrime is becoming more frequent and relevant. In your interviews with government officials, did you learn of any areas where European cyber security could be improved, and areas where it is strongest?

Boosting national cyber defense is the key. Ukraine used to be a cyber safe-haven. However, during the last few years, the NATO countries invested resources to help the country deal with cyber criminals. As a result, the country created its cyber police. Such cross-national cooperation is important, as cybercrime cannot be stopped by state boundaries.

Interview by Alexandra Gilliard

Nadiya Kostyuk is a doctoral candidate in a joint program in Political Science and Public Policy at the University of Michigan. In fall of 2017, Nadiya will be joining the Cybersecurity and Digital Technology Policy Program at the Belfer Center for Science and International Affairs of Harvard's Kennedy School as a pre-doctoral fellow. Prior to her studies, she worked as a Program Coordinator for the EastWest Institute's Global Cooperation in Cyberspace Initiative, where she currently serves as a Fellow. Nadiya's research interest are states' cyber capacities, the relationship of cybercrime to international security, and international cooperation on digital issues. She has field experiences in Bosnia and Herzegovina, China, Estonia, Ukraine, Russia, Serbia, and the Czech Republic. Currently Nadiya is working on a project mapping out the relationship between kinetic and cyber operations in Eastern Ukraine. Nadiya is a 2015 Diversity and Diplomacy Fellow and holds a master's degree in Global Affairs from New York University and a Bachelor's degree from John Jay College of Criminal Justice, where she was a McNair Scholar and Vera Fellow.

Chaos Without Coordination: an analysis of the EU's cyber (in)security

Sophie Barnett
University of Toronto

Introduction

In March 2011, the European Parliament, Commission ("EC"), and Emissions Trading Scheme fell victim to cyberattacks[1] at an approximate cost of EUR30 million in stolen emissions allowances.[2] While significant on its own, the attack represents only a small fraction of the estimated EUR85 billion that cybercrime costs the European Union ("EU") annually in addition to substantial job losses.[3] Combatting cyberattacks[4] has thus become a priority on the EU's political and security agenda. This paper explores the nature of the EU's emerging approach to addressing cyber security issues. First, it identifies the importance of achieving an effective cyber security policy in the EU. Second, it adopts George Christou's "security as resilience" approach and outlines the conditions under which an effective policy will emerge. Third, it explores current developments in EU cyber security policy and identifies three barriers to effectiveness: a lack of information sharing, the absence of common definitions, and internal divisions. This paper argues that the conditions under which such an effective cyber security policy can emerge are not yet present in the EU. Consequently, the EU remains vulnerable to cyberattacks.

Importance of an Effective Cyber Security Policy in Europe

European citizens, public services, and private businesses are heavily reliant on the internet for essential services. Thus, a common and resilient EU policy with the ability to withstand and recover from cyberattacks is crucial for ensuring public safety. The consequences of failing to do so were most pointedly exemplified by the 2007 Russian cyberattacks on Estonian computer networks, whereby government and corporate websites in Estonia were overwhelmed with data and disabled for nearly three weeks.[5] In the wake of the attack, the EU eventually published the 2010 Digital Agenda for Europe as part of the Europe 2020 Strategy, which calls for integrated responses to cyber security threats and to fight cybercrime.[6] Securing cyberspace is now recognized as a prerequisite for the EU in achieving its own objectives, protecting its citizens, and maintaining economic stability. Too much is at stake for Brussels to ignore these concerns.

In certain ways, the EU is also uniquely positioned to address cyber security issues. The transnational character of the internet implies that addressing cyber security problems at the national level is insufficient.[8] Due to the interconnectedness of civilian and military internet systems and the ease with which anyone with a computer can launch them, cyberattacks know no borders and have the potential to cause serious harm to public and private infrastructure alike.[9] As a supranational institution, the EU has the potential both to take action for the defense of European states and to serve as a role model for the world in building a global culture of cyber security resilience.[10]

A Resilient Approach to Effective Cyber Security

Until recently, there was no comprehensive, theoretically driven analysis of cyber security in Europe.[11] Christou – a Professor of European Politics at the University of Warwick and expert on EU internet governance – fills this gap by combining the concepts of resilience and security governance to construct a holistic "security as resilience" approach to assess the effectiveness of the EU's emerging cyber security policy.[12] He posits that due to the random, often undetectable, and constantly evolving nature of cyberattacks, an effective cyber security policy must necessarily be resilient: it must be proactive rather than reactive, capable of adapting to new contexts, and quick to recover from an attack.[13] Resilient cyber security policies are thus characterized by diversity, flexibility, and resistance. They rely on collaboration between state and non-state actors to create new institutions and operating procedures, thereby addressing not only the symptoms of cyber security problems but also their underlying causes.[14] Such policies allow for the best chance of preventing, withstanding, and opposing cyberattacks.

A resilient approach to cyber security starts with an understanding of the general conditions under which an effective policy can emerge.[15] Such conditions include 1) the ability and preparedness to adopt new operating assumptions and institutional structures; 2) a coalition of actors working together in partnerships based on trust to share information, construct new operating procedures, set the policy agenda, and implement new legislation; 3) convergence amongst stakeholders on a common understanding of norms and standards for a cyber security policy; 4) the evolution of a culture of cyber security at all levels of governance and among all stakeholders; and 5) an integrated approach with coherence and consistency across the policy domain.[16] For the EU to develop an effective cyber security policy, all five conditions must be present.[17] The ineffectiveness of its current approach can thus be explained by the absence of one or more of these conditions.

Barriers to Effectiveness

This section explores recent developments in EU cyber security affairs and finds that certain conditions under which an effective policy can emerge are absent. Specifically, three problems inhibit progress: 1) a lack of information sharing; 2) the absence of common definitions; and 3) internal divisions.

Lack of Information Sharing

A. EU-Member States

Information is key to the successful defense against cyberattacks and the prosecution of its perpetrators. The latter is best illustrated by Operation Payback, a distributed denial of service attack in 2013 whereby the websites of various financial service providers were targeted and disabled.[18] In this case, because the hacker was Dutch and lived in the Netherlands, national authorities were able to trace the attack, arrest the perpetrator, and bring him before a national court.[19] Yet had the hacker been of any other nationality, lived in any other state, or utilized a server located abroad, the tracing process – which is arduous to begin with – would have been significantly complicated by the fact that member states are not required to share information on cyber threats, to report security breaches to their information systems, or to cooperate with transnational investigations.[20] Consequently, pieces of the puzzle would have been missing. A further potential complication is the increased use of botnets – networks of compromised computers jointly controlled without the owners' knowledge – which also makes it difficult to distinguish between attacks originating from a specific address and those utilizing a compromised computer.[21] Hence, only by sharing information on a regular basis at the EU level can these issues be properly addressed. Failing to do so will result in all member states being vulnerable and ill-prepared to combat cyberattacks.[22]

Currently, cooperation that does occur happens largely on an ad hoc basis whereby member states exchange information when it is in their interest to do so.[23] In effect, member states often treat cyber security problems as a national security issue.[24] This is highly problematic and at odds with Christou's second condition as regulated means of communication between all actors is crucial for achieving an effective policy.[25] The EC has recognized the gap in its present capacity for sharing information:

> There is currently no effective mechanism at the EU level for effective cooperation and collaboration and for trusted information sharing on [network and information security] incidents and risks among the Member States. This may result in uncoordinated regulatory interventions, incoherent strategies and divergent standards, leading to insufficient protection against NIS across the EU.[26]

Information sharing is thus a component of the 2016 Directive on Network and Information Security ("NIS Directive"), the accompanying legislation to the 2013 EU Cyber Security Strategy: An Open, Safe, and Secure Cyberspace ("the Strategy"). The NIS Directive aims to address cyber security issues by seeking to "ensure a high common level of network and institution security across the EU."[27] It requires states to maintain a minimum level of national cyber capabilities by implementing national NIS strategies, establishing points of contact, and instituting national computer emergency response teams ("CERTs").[28] It also establishes a Cooperation Group to facilitate dialogue and information exchange between member states, the EC, and the European Network and Information Security Agency ("ENISA").[29]

Yet, while the establishment of an effective EU policy requires collaboration between actors "in partnerships based on trust to share information,"[30] the NIS Directive simply encourages

> *While the EU has previously instituted initiatives to promote private sector cooperation, a common approach for sharing information is far from constituted.*

– but does not oblige – member states to provide such information.[31] The exception to this is the requirement to forward reports from the private sector. Indeed, the NIS Directive mainly requires member states to integrate the legislation into national law to manage and monitor cyber incidents occurring within the private sector.[32] Lacking a clear obligation to communicate, the effectiveness of the NIS Directive therefore depends on voluntary cooperation from member states, who may prefer to address such problems domestically.[34]

B. EU-Private Sector

Private sector cooperation is fundamental in creating an effective cyber security policy. The reason for this is two-fold: not only do private entities utilize the same critical information systems as the public sector,[35] but they also operate much of the commercial critical infrastructure services in Europe.[36] Importantly, systematic cooperation enables the speedy exchange of pertinent information and allows for better mitigation of cyber threats. However, a framework for private sector cooperation has been developed in only five member states so far, again underlining the absence of Christou's second condition.[37]

While the EU has previously instituted initiatives to promote private sector cooperation, a common approach for sharing information is far from constituted. For example, the European Public-Private Partnership for Resilience ("EP3R"), which lasted from 2011 to 2013, was considered an "exercise in learning but which ultimately did not produce any concrete outcomes in terms of creating a sustainable platform for public and private actors to discuss and construct solutions to real problems."[38] EP3R was replaced by the NIS Public Private Platform ("NISP") in 2013, which aims to bring together public and private stakeholders and identify good practices to tackle cyber security risks.[39] However, it has yet to be implemented and scholars have already questioned its capacity to build the "necessary trust and regular interaction needed"[40] for sufficient information sharing.

The NIS Directive addresses information sharing by requiring "operators of essential services" – public and private entities in the energy, transport, banking, financial, health, water supply, and digital infrastructure sectors providing a service that is "essential for the maintenance of critical activities"[41] – to notify relevant national authorities of incidents impacting the services they provide.[42] However, it tasks individual states with identifying operators for inclusion under these provisions and thus results in inconsistencies across member states.[43] Companies selected for inclusion may fear the business repercussions of sharing such information, and if information is withheld, national authorities may be unable to prove non-compliance if they are unaware that the cyberattack has occurred in the first place. These circumstances potentially compromise the efficiency of information sharing initiatives.

In addition, a fundamental disconnect exists in the flow of information under the NIS Directive as the private sector must report breaches through national authorities which in turn forward the information to EU institutions. This slows down the delivery process and may hinder timely access to crucial information. Because cyberattacks are difficult to prevent, states must act quickly upon detection to avoid damage.[44] Given the shared use of information systems, an inefficient delivery process may be the difference between causing minor setbacks to a system and a hugely destructive outcome with consequences felt far beyond the victim company. A further gap exists in the identification of the information that a company must report. While the NIS Directive requires the reporting of a "major threat to the functioning of network or information systems,"[45] it fails to define such threats and instead leaves the determination to member states, ENISA, CERTs, or the Cooperation Group.

Absence of Common Definitions

For an effective policy to emerge, Christou's third condition requires stakeholders to share a common understanding of its norms and standards.[46] Here, the EU lacks a common definition of "cyber security" and the events that constitute a cyberattack.[47] Although ENISA has recognized this problem and provided its own definitions, their descriptions are not common across the EU, and both the Strategy and the NIS Directive – which are common – fail to clarify these terms.[48] Consequently, member states and EU institutions are left to their own interpretations. There is also no clear distinction between various forms of cyberattacks with terms often used interchangeably to refer to the defense against any and all of cyber warfare, cyberterrorism, cyber espionage, cyber intrusion, or cybercrime.[49] Furthermore, no differentiation exists between cyberattacks occurring between private individuals, between states, or between states and private individuals.[50] This results in another problem: Without clear distinctions in terminology, it is unclear which EU institution should manage a particular situation or whether the issue should even be addressed at the member state or EU level in the first place.[51]

Internal Divisions

A. EU-Member States

Christou's fourth condition requires there to be a common culture of cyber security at all levels of governance and among all stakeholders.[52] Such a culture does not yet exist within the EU. Differences in national policies and defense capabilities prevent the establishment of a common approach to cyber security issues.[53] While 15 member states have introduced a distinct cyber security strategy, others have simply added a cyber dimension to existing national security strategies, and some have not addressed cyber security issues at all.[54] This is partially a result of the fact that member states must define cyber security individually and thus their assessment of cyber threats differ. For example, Estonia focuses on securing the systems on which it is highly dependent.[55] It recommends various civil measures and focuses on regulation, education, and cooperation.[56] Concurrently, the United Kingdom much more broadly calls to tackle cyber threats from criminals, terrorists, and states to make cyberspace safe for citizens and business.[57]

The Strategy marked the EU's first attempt to establish a common cyber security policy.[58] However, it failed to address these contradictions.[59] The Strategy outlines five priorities: 1) achieving overall resilience, 2) fighting cybercrime, 3) developing cyber defense policy and capabilities, 4) developing industrial and technological resources, and 5) establishing an international policy to promote core EU values.[60] However, none of these priorities can be achieved without first establishing internal consensus on how to approach them. Even when consensus is reached, it will take time for the priorities to take root in the political culture of the EU. In the meantime, different member states inevitably will prefer different mechanisms for responding to cyberattacks, making it hard to reach consensus on what a common policy entails.[61] The longer these divides continue, the longer it is that member states leave the EU "toothless" in the case of future attacks.

B. EU Institutions

Christou's fifth condition requires a coherent, integrated, and consistent approach to addressing problems in cyber security across the policy domain.[63] However, fragmentation is a huge problem between EU institutions. While there are many institutions addressing cyber security issues in the EU, there is no single point of policy coordination between them.[64] A Cybersecurity Coordination Group was established in 2011, but it only functions as a technical point of coordination translating policy into standards containing technical details and not as a coordination point for policymaking and collaborative action.[65]

The number of uncoordinated institutions involved in EU cyber security policy produces complications in differentiating their respective mandates and thus determining which institution should act in each circumstance.[66] For example, the Directorate-General ("DG") for Communications, Networks, Content and Technology issued the Digital Agenda for Europe in 2010, which included the creation of a common cybercrime platform.[67] Yet, Europol's Cyber Crime Centre ("EC3") appears to create overlapping jurisdiction as it aims to broaden and incorporate further expertise in specialized areas.[68] Concurrently, the DG for Migration and Home Affairs addresses policy issues concerning cybercrime and works with Europol, ENISA, and EC3,[69] while the European Defence Agency ("EDA") works with the EU Military Staff ("EUMS") to improve cyber defense capabilities.[70] In addition, the DG for Enterprise and Industry conducts research and development on how to best protect European citizens from harm emanating from cyber threats.[71] The European External Action Service serves as the EU's diplomatic agent and acts as a coordinator between EU and non-EU cyber security strategies,[72] while ENISA aims to enhance the capabilities of the EU, member states, and the private sector to address network and information security problems.[73]

In response to this fragmentation, the EU launched the Strategy in part to clarify institutions' roles and responsibilities.[74] It stated that ENISA offers a platform for member state cooperation over cyber security and achieving cyber resilience; EC3, Eurojust, and Eurpol work to fight cybercrime; and EDA and EUMS aim to improve cyber defense capabilities.[75] However, this clarification did not offer new solutions to existing problems. As the European Cyber Security Protection Alliance reports, the Strategy has largely failed to reduce institutional fragmentation:

> Currently, there is an impressive collection of directives, organisations, policies and the like, which makes it difficult to instantly and fully grasp how this broad topic is addressed within the EU. The fragmented and intransparent approach manifests itself in the [Strategy] which is … not (yet) able to singlehandedly take on the role of a general European cyber security strategy as it lacks some essential aspects of what makes a strategy effective.[76]

Thus at present, there are too many actors involved in the EU's cyber security domain and too little harmonisation among them. If the EU is to establish an effective policy, it must create a single point of policy coordination and clarify the respective responsibilities of all relevant institutions. Combined with the lack of information exchange and common definitions, fragmentation further challenges the EU's ability to address cyber security problems proactively by adopting new operating assumptions as required which, as previously established, is Christou's first condition for the creation of a resilient cyber security policy. Without effective communication, unity, and coordination, it is difficult to decipher when and how such assumptions would necessarily be developed and which institution would lead the process in a particular situation.[77]

Conclusion

With the speed of technological innovation and Europe's increasing reliance on the internet, both the threat and scale of cyberattacks are likely to increase. But while the EU's cyber security policy continues to evolve, it remains complicated and ineffective. There exists a lack of common understanding and decisive cooperation between EU institutions, member states, and the private sector, thus inhibiting the emergence of an effective cyber security policy and leaving all actors vulnerable in cyberspace. If the EU is to establish an effective cybersecurity policy, it must first achieve internal coherence and consensus on the details of a common vision.

Sophie Barnett is a fourth-year student pursuing an Honours BA in international relations at the University of Toronto. She has research interests in both cybersecurity and forced migration, with a regional focus on Europe and the European Union. Sophie is the Co-Chair of the G20 Research Group and serves as a research assistant for Dr. John Kirton at the Munk School of Global Affairs. Her work has been featured by a variety of sources, including E-International Relations, the NATO Association of Canada, and the University of Southern California International Review.

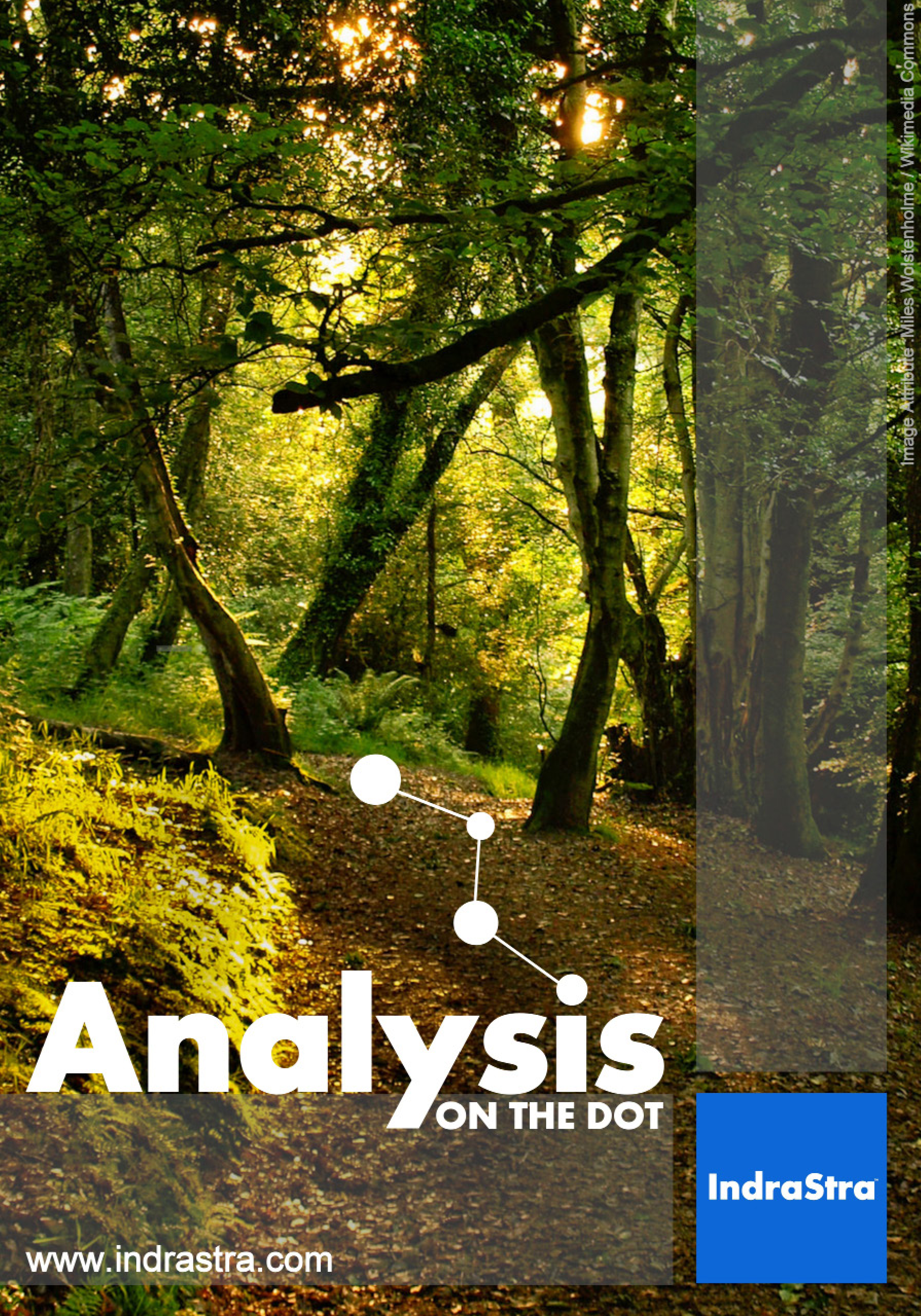


Image Attribute :Miles Wolstenholme / Wikimedia Commons

Analysis

ON THE DOT

IndraStra™

www.indrastra.com

The Thin Line Between Utopia and Dystopia: policing child porn on the Darknet

Jordan Cohen
Georgetown University

The Deep Web is the section of the World Wide Web that is not indexed by search engines like Google and Bing. The spotlight and the general public's interest did not switch onto this part of the Internet until 2013, when the FBI took down the Silk Road marketplace (which was part of the Darknet, a nuance lost on many[1]) and exposed the Internet's notorious drug-trafficking underbelly. It is worth noting that this cyber-frontier is intrinsically neither good nor bad but it holds particular attraction for pioneers because its resources haven't been fully explored. The Deep Web appears to be larger than the territory that's already been settled but genuine outposts of activity are probably quite sparse and widely separated. Because of its nature, it's impossible to determine the number of Deep Web pages and content at any given time or to provide a comprehensive picture of everything that exists in it — no one can say with certainty that they have fully explored its depths. Estimates vary, but many agree that the Deep Web is 500 times larger than the Surface Web, and only a small portion of that is dedicated to criminal enterprise — the rest is mundane or empty.[2]

What is criminal enterprise on the internet? Cybercrime, a vague and seemingly indefinable catchall phrase, flourished in the first decade of the 21st century, especially in the Post-Soviet region, on clear web websites and forums like *Carders Market*. During this nascent period, filled with phishing, fraud, laundering, Distributed Denial of Service (DDOS) attacks, malware, ransomware, theft, and transaction of illegal or pirated goods and technology, cybercrime rapidly evolved from the domain of misguided pranksters, to elaborate profit-driven schemes involving organized-crime syndicates that may be based anywhere in the world. A portion of this large and diverse criminal ecosystem has moved into the small corner of the Deep Web, into a subset of the Dark Web, called the Darknet/Darkmarket, where fundamental things like who you are and where you or the website you are using is located are purposely kept secret for criminal means.[3] This is the domain created by tools like (mainly) Tor and I2P that provide ways to interact that are difficult to discover, and are relatively anonymous and untraceable. Among its many other uses, it can be a gathering point for communities who want to engage in things like robbery/assassinations to order, sex trafficking, arms trafficking, terrorism, drug selling/buying, laundering, doxxing services, counterfeiting, and, perhaps most disturbingly, distributing child pornography.

The origins of Tor go back to 1995, when, funded by the ONR (Office of Naval Research) and DARPA (Defense Advanced Research Projects Agency), military scientists Paul Syvverson, Michael Reed, David Goldschlag, and later Roger Dingledine began developing a partially decentralized cloaking technology that would prevent someone's activity on the Internet from being traced back to them. They called it "onion routing," a method redirecting traffic into a parallel peer-to-peer network and bouncing it around randomly before sending it off to its final destination. The idea was to move the packets as they traverse around so as to confuse and disconnect its origin and destination, and make it impossible for someone to observe who you are or where you are browsing on the Internet. In their seminal 2004 paper, the scientists released The Second-Generation Onion Router which, through "perfect forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services via rendezvous points," provided "a reasonable tradeoff between anonymity, usability, and efficiency." This privacy by design has attracted a critical mass of users, averaging two million per day as of June 2015 — an impressive number, even though the service does not provide the absolute impunity that is often attributed to it. Because of its novelty (at this stage many experts and analysts are still just finding out what's going on rather than who is doing it) and other complex challenges, law enforcement and policy makers question how best to contend with evolving technology such as encryption and the challenges of attribution in an anonymous environment to effectively combat malicious actors who exploit cyberspace, including the Dark Web. Examining the case of the proliferation of child pornography on the Dark Web via Tor will guide policy makers as to how to confront cybercrime on the largely anonymous Dark Web in a nuanced, balanced, and creative manner.

There are a plethora of reasons why people would want to remain relatively anonymous or set up sites that cannot easily be traced back to a physical location or entity – it can be a safe haven and a secure communication channel for citizens under restrictive regimes, journalists and whistle-blowers.[4, 5] Nevertheless, for the worst criminals it is the safest place to conduct their business online. Adding to this, most experts agree that online criminal communities, especially those based around illegal sexual violence, experience a psychology that includes feelings of dissociative anonymity, invisibility, asynchronicity, solipsistic introjection, dissociative imagination, and minimizing authority, which all become motivating factors to "dig themselves deeper" into criminal elements.   Instead of fueling blanket cyberphobia, policies should be crafted to contexts specified by ethnographic analysis and empirical programs of research that are sensitive to the diverse contexts of the web: a mapping of the hidden services directory, customer data monitoring, social site monitoring, hidden service monitoring, marketplace profiling, and semantic analysis. When it comes to cybercrime versus the criminal's use of cyberspace, we must balance two realities: chasing the chimeras of our fevered imaginations while watching the information flows where the real action is taking place — all the while utilizing the valuable information of Deep Content.[6]

Between December 2000 and June 2014, the estimated number of Internet users grew from almost 361 million to nearly 7.2 billion—an increase of more than 741%. Notwithstanding the radical changes in the character of the Internet over the last two decades, one constant has remained of concern for many users and regulators of the medium: the popularity of this "Internet Babylon" amongst those who wish to disseminate illegal pornographic materials – especially those depicting and exploiting children – on what was once described as 'the biggest dirty bookshop in history." Nevertheless, statistics are elusive and many times faulty when it comes to determining how much illegal porn is on hidden services somewhat protected by Tor. One oft cited study on the matter, from the Global Commission on Internet Governance, examined Tor traffic to hidden services. while about 2% of the Tor hidden service websites identified were sites that researchers deemed related to child abuse, 83% of the visits to hidden services sites were to these child abuse sites—"just a small number of pedophilia sites account for the majority of Dark Web http traffic." As has been noted, however, there are a number of variables that may have influenced the results and they should be taken with a grain of salt.[7] Regardless, among the range of underground and emergent sub-cultures, the one that is universally agreed upon to be the most repulsive, is child pornography (CP).[8] According to the Internet Watch Foundation 68,092 cases were confirmed as online child exploitation in 2015, which is a 118% increase from 2014. 34% of that content is category A and 70% of victims assessed as ten or under.[9] Law enforcement and the cyber community have taken action though, and a 150% increase in takedown notices issued for newsgroups containing child sexual abuse imagery in 2015 is a testament to that.[10] When visitors accessed a CP site on the Darknet, Playpen, for example, the FBI masterfully deployed a network investigative technique (NIT) – a hacking tool – and used a single warrant to uncover 1,300 IP addresses, tracing these addresses back to actual individuals.[11] Although the act undoubtedly helped to bring down child pornographers, the American Civil Liberties Union is concerned that the FBI was able to obtain computer IP addresses of over 1,000 computers with just a single warrant. What comes to the average computer user, not likely to ever want or need to use Tor, is a modern dilemma: He/she wants personal freedom and encryption, not dragnet surveillance, but they also do not want safe havens for pedophiles. Additionally, citizens do not want to make an absolute trade between these things. Clearheaded policy proposals can help ameliorate the rocky balance between surveillance and darkness in the world of Tor.

Law enforcement's successes in the field already should be lauded. A challenge one finds when exploring the evolution of media law is that technologies, and child abusers ability to circumvent surveillance, develop more rapidly than the concomitant legal framework. In addition, in the case of online child exploitation, police usually cannot incarcerate leaders or agitators, making it difficult to destroy infrastructures.

The institutions of the porn trade are neither fixed nor localized; rather it seems that the goal should be reducing the problem to trivial proportions. Like the rest of the Deep Web, the first step is to find out what is happening. Strides are being made in that direction. The Department of Defense's (DOD) DARPA is conducting a research project called Memex to develop a new search engine that can uncover patterns and relationships in online data to help law enforcement and other stakeholders track illegal activity. The Memex project ultimately aims to build a more comprehensive map of Internet content. Teamed with new investigatory techniques, such as the sophisticated forensic examination of storage devices, close work with Internet Service Providers (ISPs), humanitarian NGOS, and vigilante organizations, the United States' law enforcement is beginning to understand that the biggest single problem facing police is simply recognizing and understanding the nature of the Child Porn world on the Net. Significant victories have been achieved. There have been mass raids and arrests, some of which have broken up major CP rings, and operations have demonstrated an impressive degree of international coordination. It is imperative that the US Intelligence community continues efforts to develop international consensus on norms about how to deal with cases where the goal of protecting data comes into conflict with the requirements of law enforcement or security agencies to investigate the exploitation of children online.

Despite all the enforcement efforts of recent years, it is still remarkably easy for any reasonably discreet person to pursue this highly illegal conduct indefinitely, as long as obvious traps are avoided. This does not mean that police have been lackadaisical or incompetent, still less that their hands have been tied by legislators. Hitherto, law enforcement agencies and political officials have had a very poor idea of the organization and mechanisms of the CP subculture, and above all, of its critical institutions such as the newsgroups and bulletin boards. Given the public loathing of CP and the support that could be mobilized against it, it is incredible that virtually nobody outside the subculture is aware that this community even exists in the specific capacity it does. That may be changing though, this year, the National Center for Missing and Exploited Children (NCMEC) received 4.4 million reports to its CyberTipline. That's a nearly 800% increase in reporting since 2013. Former Secretary of Homeland Security Michael Chertoff recommends law enforcement to continue trying to map the hidden services directory as well as mobilizing data monitoring, social site monitoring, and hidden service monitoring. Once a hidden service has been discovered it needs to be understood and properly categorized, through semantic analysis — optimally automatically — in terms of the concepts and relationships they represent and not simply the words they contain. These widely abused platforms — in sharp contrast to the wider public-key infrastructure — are and should be fair game for the most aggressive intelligence and law-enforcement techniques, as well as for invasive academic research. Refusing to confront tough and inevitable political choices and ignoring child exploitation is simply irresponsible. In the words of security consultant Mark Stockley, "the line between utopia and dystopia can be disturbingly thin." Law enforcement will have to tread this line carefully, making sure they are actively balancing the alarming realities at hand, with the rest of the law-abiding population's rights.

In the context of the regulation of anonymous services via Tor and the lack of formal, state-led regulation (due to the aforementioned "failure for technological reasons of the enforcement of/impact by traditional laws/law enforcement mechanisms, the relative novelty of the technology itself, and the consequent impact of this absence upon prevailing attitudes upon this particular environment") a new regulatory paradigm should acknowledge community-led regulation as a supplementary entity (potentially including but not limited to the Anonymous group's activities discussed previously in the footnote above). This may be, in Murray's terms, a less disruptive form of regulation and "without the support of a base of regulatees, the prospects for a dynamic regulatory intervention are poor." A multifaceted approach has at least the potential to be more effective in relation to the regulatory task at hand than an imposed regulatory model, with solely state-led enforcement mechanisms, that may, due to the difficulty in reaching the relevant virtual environment, swing and miss.

Cyber and physical space blur. In addition to developing technology to infiltrate and deanonymize services such as Tor, law enforcement may rely upon more traditional crime fighting techniques; some have suggested that law enforcement can still rely upon mistakes by criminals or flaws in technology to target nefarious actors. For instance, in the Silk Road takedown "missteps" by the site's operator revealed his own physical location and led to the (first iteration of the) marketplace's demise. While Internet CP has become "the quintessential global crime problem", it remains a fundamentally local problem and raises serious questions about risks of actual contact abuse posed by those arrested for accessing or possessing child pornography. Pursuit of Internet groomers and other Dark Web offenders should not overshadow efforts to prevent contact child abuse itself. There are certain strategies that have been originally overlooked, like targeting and contacting young people about risky behavior online

> *A full 95% of the deep Web is publicly accessible information — not subject to fees or subscriptions also appear to be the fastest growing information component of the Web. Serious information seekers can no longer avoid the importance or quality of deep Web information.*

so as to give them tools to be equipped when an abuser gestures for them to meet. Another simple, but straightforward idea that is percolating in academic circles is alerting detected users immediately, rather than emboldening an abuser through an undercover conversation. These are becoming more popular and with recent work by DARPA for example, by creating a more comprehensive look into the Deep Web, a balanced[12] future does look possible.

Until Van Leeuwenhoek first looked at a drop of water under a microscope in the late 17th century, people had no idea there was a whole world of "animalcules" beyond their vision. Deep-sea exploration in the past thirty years has turned up hundreds of strange creatures that challenge old ideas about the origins of life and where it can exist. Discovery comes from looking at the world in new ways and with new tools. The mysterious Deep Web and Darknet child pornography are both topics that generate strong emotions. Because a microscope has not been created yet, there are so many unknowns. Nevertheless, along with strong reactions to these fields comes the danger of blanketed and polarized views. In our fervent desires to "do something" about the relative CP safe haven of the Darknet, we risk falling victim to a moral panic where cyberphobia fuels either an urge to infiltrate and/or destroy the whole institution or for cyber libertarians, to raise the flag of total privacy.

While the psychological and physical effects that child exploitation on Tor has on its victims are devastating and morally indefensible, and a targeted and aggressive monitoring regime is necessary, the "animalcules" of this loathsome community should not paint the rest of the deep- Sea. If the most coveted commodity of the Information Age is indeed information, then the value of Deep Web content is immeasurable. Deep Web content is highly relevant to every information need, market, and domain. A full 95% of the deep Web is publicly accessible information. Serious information seekers can no longer avoid the importance or quality of deep Web information. At these early stages, we must treat with caution claims about the size of the CP problem and separate our moral outrage from the exploiters in order to understand community behavior and deviant decision making processes. Through this multidisciplinary approach, law enforcement will be on the road to prevent CP offenses before they occur, all the while recognizing the amazing potential of the rest of the Deep and Dark Web.

Jordan Cohen is a fourth-year student in the Bachelor of Science in Foreign Service BSFS/SSP 5 year M.A. program at Georgetown University's School of Foreign Service. His studies focus on International Security and his interests include organized crime, money laundering, trafficking, insurgency, and terrorism.

REFERENCES AND FOOTNOTES

POPULISM IN THE DIGITAL AGE

Tracing the transformation of Populism in Europe and America

[1] John Abromeit, "Transformations of Producerist Populism in Western Europe," Transformations of Populism in Europe and the Americas: History and Recent Tendencies, eds. J. Abromeit, B. Chesterton, G. Marotta and Y. Norman (London: Bloomsbury Academic, 2016), 231-64.

[2] On Sieyes and his pamphlet, see William Sewell, A Rhetoric of Bourgeois Revolution: The Abbé Sièyes and What is the Third Estate? (Durham and London: Duke University Press, 1994).

[3] On Sorel and his fascist reception, see Zeev Sternhell, The Birth of Fascist Ideology: From Cultural Rebellion to Political Revolution, trans. David Maisel (Princeton: Princeton University Press, 1994) and Neither Left Nor Right: Fascist Ideology in France, trans. David Maisel (Princeton: Princeton University Press, 1986).

[4] David Roediger, Wages of Whiteness: Race and the Making of the American Working Class, Revised Edition (London and New York: Verso, 2007), 59-60.

[5] Richard Hofstadter, The Age of Reform: From Bryan to F.D.R. (New York: Vintage, 1955).

[8] On the "bloody era in populist historiography" see Gary Marotta, "Richard Hofstadter's Populist Problem and his Identity as a Jewish Intellectual," Transformation of Populism in Europe and the Americas, op. cit., 105-15.

[7] Charles Postel, The Populist Vision (Oxford, Oxford University Press, 2007). For Postel's critique of the "Hofstadter thesis," see also his essay "The American Populist and Anti-Populist Legacy," in Transformations of Populism in Europe and the Americas, 116-35.

[8] Theda Skocpol and Vanessa Williamson, The Tea Party and the Remaking of Republican Conservatism (Oxford: Oxford University Press, 2012), 64-68.

[0] See, for example, Nate Cohn, "A 2016 Review: Turnout Wasn't the Driver of Clinton's Defeat," New York Times, March 28, 2017. https://www.nytimes.com/2017/03/28/upshot/a-2016-review-turnout-wasnt-the-driver-of-clintons-defeat.html?_r=0

[10] See, for example, Trump speech in Rochester, New York on April 10, 2016: https://www.youtube.com/watch?v=NqRMaD3HWHo

[11] Thomas Piketty, Capital in the Twenty-First Century, trans. Arthur Goldhammer (Cambridge, MA: Harvard University Press, 2014) and Joseph E. Stiglitz, The Price of Inequality: How Today's Divided Society Endangers our Future (New York: Norton, 2012).

[12] Leo Lowenthal and Norbert Guterman, Prophets of Deceit. (New York: Harper & Brothers, 1950).

[13] Theodor Adorno, et. al. The Authoritarian Personality (New York: Harper & Brothers,1950), 675-85.

[14] Ibid., 676.

Trump's Tea Party

References:

Arrillaga, Pauline. 2012. "Tea Party 2012: A Look at the Conservative Movement's Last Three Years." *The Huffington Post,* April 14. Retrieved April 14, 2013 (http://www.huffingtonpost.com/2012/04/14/Tea-party-2012_n_1425957.html).

Bischoff, Laura A. and Mallow, Daniel. 2012. "GOP Convention to Show Tea Party Influence." *The Atlanta Journal – Constitution*. August 26th. Retrieved March 9th, 2013 (http://www.ajc.com/news/news/local/gop-convention-to-show-tea-party-influence/nRMSZ/)

Boot, Max. 2016. "How the 'Stupid Party' Created Donald Trump." *The New York Times*. July 31st. Retrieved March 22nd from https://www.nytimes.com/2016/08/01/opinion/how-the-stupid-party-created-donald-trump.html.

Boykoff, Jules and Laschever, Eulalie. 2011. "The Tea Party Movement, Framing, and the U.S. Media." *Social*

Movement Studies. 10(4): 341-366.
Burstein, Paul. 1999. "Social Movements and Public Policy." Pp. 3-21 in How Social Movements Matter, edited by Marco Giugni, Doug McAdam, and Charles Tilly. University of Minnesota Press
Greenhouse, Steven. 2011. "Strained States Turning to Laws to Curb Labor Unions." *New York Times*. January 3rd. Retrieved on March 11th, 2013 (http://www.nytimes.com/2011/01/04/business/04labor.html?pagewanted=all&_r=0)
Hair, Corbin. 2010. "How the Tea Party Utilized Digital Media to Gain Power." *Media Shift*. Retrieved March 22nd, 2017 from http://mediashift.org/2010/10/how-the-tea-party-utilized-digital-media-to-gain-power301/
Hoftsadter, Richard. 1963. *Anti-intellectualism in American Life*. New York: Vintage Books.
McAdam, Doug. 1994. "Social Movements and Culture." pp. 36-57 in Joseph R. Gusfield, Hank Johnston, and Enrique Larana (eds.), *Ideology and Identity in Contemporary Social Movements*. Philadelphia, PA: Temple University Press.
Pew Research. 2017. "Social Media Fact Sheet." Pew Research Center. Retrieved on March 23rd, 2017 from http://www.pewinternet.org/fact-sheet/social-media/.
Raynauld, Vincent. 2013. "The perfect political storm? The Tea Party movement, the redefinition of the digital poltical mediascape, and the birth of *online politicking 3.0*." Dissertation. Carleton University, Ottawa, Ontario.
Rochon, Thomas R. 1998. *Culture Moves*. Princeton, NJ: Princeton University Press.
Thompson, Derek. 2010. "The Tea Party Used the Internet to Defeat* the First Internet President". *The Atlantic*. November 2nd. https://www.theatlantic.com/business/archive/2010/11/the-tea-party-used-the-internet-to-defeat-the-first-internet-president/65589/
Zernike, Kate. 2010. *Boiling Mad: Inside Tea Party America*. New York: Times Books.

Populism Down Under: The rise, fall, and resurgence of Pauline Hanson and the One Nation Party

Footnotes:

[1] Currently each state is represented by 12 senators, while the Norther Territory and the Australian Capital Territory are each represented by two senators. Currently each state is represented by 12 senators, while the Norther Territory and the Australian Capital Territory are each represented by two senators.

[2] There have only been seven double dissolutions in Australia since 1901.

[3] The Australian Greens first won a lower house seat in 2010; the Palmer United Party won a lower house seat in 2013; the Nick Xenophon Team won a lower house seat in 2016.

[4] This was due to the government's desire to increase the House of Representatives from 125 to 148 members, triggering the 'nexus' provision in the Constitution which requires that the number of House of Representative districts be, as close as possible, double the number of senators. Currently, there are 150 lower house seats while there are 76 seats in the Senate: 12 from each state and two each from the Northern Territory and the Australian Capital Territory.

[5] Australia had a double dissolution election in 2016 where all Senate seats were up for election which meant that the quota required to win representation was half that required during an ordinary general election.

References:

Australian Motoring Enthusiast Party. 2013. Core values. Retrieved at: http://www.australianmotoringenthusiastparty.org.au/core_values
Betz, H. 1993. The new politics of resentment: radical right wing populist parties in Western Europe. *Comparative Politics*. 25, 4: 413-427.
Betz, H. 1998. Introduction. In *The New Politics of the Right*. Edited by Hans-Georg Betz and Stefan Immerfall. Houndmills:Macmillan. 1-10.
Butcher, J. 2014. Make or break? The peril of political promises. *Canberra Times*. May 8. Retrieved at: http://www.canberratimes.com.au/comment/make-or-break-the-peril-of-political-promises-20140505-zr4q9.html
Crime and Misconduct Commission. 2004. *The Prosecution of Pauline Hanson and David Ettridge: A Report on an Inquiry into Issues Raised in a Resolution of Parliament*. Brisbane: Crime and Misconduct Commission.
Duverger, M. 1954. *Political Parties*. New York: Wiley.
Economou, N. 2015. The environment in the 2013 election: controversies over climate change, the carbon tax and conservation. In *Abbott's Gambit: The 2013 Australian Federal Election*. Edited by Carol Johnson and John Wanna. Canberra: ANU Press. 341-358.
Gothe-Snape, J. 2016. War of words erupts between Pauline Hanson and Malcolm Turnbull. *Daily Telegraph*. May 31.

Retrieved at: http://www.dailytelegraph.com.au/news/national/federal-election/war-of-words-erupts-between-pauline-hanson-and-malcolm-turnbull/news-story/829ad707087a0cd4bd82a32a163e5ef5

Green. A. 2013. The growth in the number of registered political parties. *ABC Elections*. December 2016. Retrieved at: http://blogs.abc.net.au/antonygreen/2013/12/the-growth-in-the-number-of-registered-political-parties.html

Hainsworth, P. 2000. *The Politics of the Extreme Right: From the Margins to the Mainstream*. London: Pinter.

Hanson, P. 1996. *Commonwealth of Australia Parliamentary Debates*. Canberra: House of Representatives.

Kingston. M. 2007. "Margo Kingston reviews Pauline Hanson's autobiography." *The Book Show*, April 30. Sydney: ABC Radio National. Retrieved at: http://www.abc.net.au/radionational/programs/bookshow/margo-kingston-reviews-pauline-hansons/3238802

Liberal Democrats. 2016. Taxation policy. Retrieved at: https://ldp.org.au/policy/taxation/

Mughan, A., Bean, C. and McAllister, I. 2003. Economic globalization, job insecurity and the populist reaction'. *Electoral Studies*. 22, 4: 617-633.

Nelson, P. 2010. "Socio-economic indexes for 2009 electoral divisions: 2006 Census." *Parliament of Australia Research Paper 1* (2010-2011). Retrieved at: http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1011/11rp01#_Toc205175229

Pauline Hanson's One Nation. 2016a. One Nation policies: Islam. Retrieved at: http://www.onenation.com.au/policies/islam

Pauline Hanson's One Nation. 2016b. One Nation policies: Halal certification. Retrieved at: http://www.onenation.com.au/policies/halal-certification

Pauline Hanson's One Nation. 2016c. One Nation policies: Economics and tax policy. Retrieved at: http://www.onenation.com.au/policies/economics

Riker, W.H. 1986. Duverger's Law revisited. In *Electoral Laws and their Political Consequences*. Edited by Bernard Grofman and Arend Lijphart. New York: Agathon Press. 19-42.

Salt, B. 2017. Pauline Hanson rides spirit of times as bush-city divide widens. *The Australian*. April 6. Retrieved at: http://www.theaustralian.com.au/business/opinion/bernard-salt-demographer/hanson-rides-spirit-of-times-as-bushcity-divide-widens/news-story/093a32f69a8b66226fdc0a50436d3f1b

Sawer, M. 2004. Above-the-line voting: how democratic? *Democratic Audit of Australia*. Retrieved at: http://democratic.audit.anu.edua./abovetheline.pdf

Media, Web, Democracy: Populist and Post-populist Europe in the Mirror of the Italian Experience

Footnotes:

[1] MSM- the mainstream media- asLe Monde,Libération, El Pais,FAZ,Financial Times,Spiegel, The Economist. These organisations are as well classified as populists by a large number of scholars investigating populism: see, i.e., Yves Mény and Yves Surel, 2002, Geoff Andrews, 2005.

[2] Eco, U. 2007. Turning Back the Clock: Hot Wars and Media Populism. Boston: Houghton Mifflin Harcourt. The well known semiologist disappeared in 2016.
According to the journalist Lorraine Berry, Umberto Eco's essay Ur-Fascism, written in 1995 for the New York Review Book, which teaches how to recognize fascism, is very useful in order to look at the phenomenon Donald Trump. http://lithub.com/umberto-eco-on-donald-trump-14-ways-of-looking-at-a-fascist/

[3] http://blogs.lse.ac.uk/europpblog/2016/06/22/the-five-star-movements-victories-in-italys-mayoral-elections-a-major-blow-for-renzi-and-the-pd/#Author

[4] The Austrian Freedom Party (FPÖ) was founded in 1956 by Anton Reinthaller, a former Nazi Minister of Agriculture and SS officer.

[5] Italian neo-fascism is composed of a constellation of small parties, movements, cultural associations, and football (soccer) supporters' clubs that are often tempted by hooliganism. Their lowest common denominator is in the assumption of ideological elements, behaviors, languages, and symbols of Nazism and fascism. Each of these groups makes an arbitrary selection among these elements, choosing the ones that most appeal to its members that use them to build a specific identity. Neo-fascist groups use mainly the Web to communicate their messages and to induce new followers (Caiani, M. and Parenti, L. 2013).

[6] Berlusconi did not easily accept the Maastricht budget constraints, searching consensus on promises of redistribution (the abolition of a tax on the home, for example).

[7] The Forward Italy MPs are still sitting together with the German Christian democrats of Angela Merkel

[8] Berlusconi owned three channels, which made him an immense fortune. He is still enourmously rich: in 2016, Forbes magazine ranked him as the 188th richest man in the world with a net worth of US$7.1 billion (Forbes, 2011).

[9] Berlusconi tried to impose some classical measures of the neo-liberal agenda: to reduce the power of the trade unions and the workers' guarantees; to shrink the welfare; to privatise public services; to impose a stronger control of migration (mainly under the pressure of the Northern League). To conclude, much of Berlusconi's political program was not different from the one of the traditional European right. The attempts on controlling the independence of the justice system regularly failed (Friedman 2015).

[10] Still, in 2013, when the last general elections took place, for Italians, the television was still the primary tool for staying informed (51.9%); in second place, with a wide gap, are placed the online newspapers (18.1%), then blogs and other websites of information (10.9%), daily paper (9.4%), radio (8.1%), and the free press (1.6%) (Eurispes Report 2013).

[11] Direct democracy is a complex idea. There are two concepts that are mixed. The first is that the people should decide and not delegate: you need to extend the number of people who actually take the decisions. This is the deliberative democracy designed by Jürgen Habermas. The other concept is the involvement of citizens in the entire decision-making process: they should not only say a yes and a no at the end. The ideal would be to combine both factors.

[12] https://www.meetup.com

[13] http://www.ilblogdellestelle.it/votazioni_di_oggi_su_rousseau.html

[14] In his book *On Populist Reason* Ernesto Laclau (2005: 67) argues that populism is the 'royal road to understanding something about the ontological constitution of the political as such'. By this he means that through an understanding of the oft-denigrated phenomenon of populism we can grasp some of the fundamental discursive operations of all politics.

[15] He also did a few measures that brought consensus as abolishing taxes on the first home (in a country where house propriety is spread).

[16] As a matter of fact, European technocrats – and politicians of the most powerful EU countries – have assumed that democratic governments in crisis countries had lost the capacity to deal with the key problems of their economies and societies, imposing non-elected technocratic governments in Greece and Italy. The role of the EU in this shift towards elitarian technocratic oligarchy has caused growing Euroscepticism all over, even in countries that had not been deeply touched by the crisis, as the Brexit vote shows.

[17] The European Union economic dogma is opposed to Keynesian economy, prohibiting states from deficit spending that could boost the economy.

References

Adinolfi, M. 2012: Grillo imputato assomiglia a Silvio. *l'Unità*. 4 May. Available at: http://www.unita.it/italia/beppe-grillo-imputato-no-tav-br-gli-stessi-argomenti-di-silvio-1.407464 [accessed 12 September 2016].

Albertazzi, D., McDonnell, D. (Eds.) (2008), *Twenty-First Century Populism*
The Spectre of Western European Democracy, Palgrave Mac Millan, London

Andrews, G. 2005. *Not A Normal Country: Italy After Berlusconi*. London: Pluto Press.

Caiani, M. and Parenti, L. 2013. *Web nero*. Bologna: Il Mulino.

Caldiron, G. 2001. *La destra plurale. Dalla preferenza nazionale alla tolleranza zero*. Bologna: Manifestolibri

Campani G. (2016), Neo-fascism from the Twentieth Century to the Third Millennium: The Case of Italy in Campani G. Benveniste, A. Lazaridis, G. (2016a)The Rise of the Far Right in Europe, Populist Shifts and 'Othering', Palgrave, Macmillan, London, pp. 25-54

Della Porta, D. and Mosca, L. 2006a. Democrazia in rete: stili di comunicazione e movimenti sociali in Europa. *Rassegna Italiana di Sociologia*, 4(Oct-Dec), 529–56.

Della Porta, D. and Mosca, L. 2006b. *Democracy in the Internet: a presentation*. Report on Work Package 2 of the Project Demos (Democracy in Europe and the Mobilization of Society).

Diamanti, I. 1993. La Lega. *Geografia, storia e sociologia di un nuovo soggetto politico*. Roma: Donzelli.

Diamanti, I. 1996. I*l male del Nord. Lega, localismo, secessione*, Roma: Donzelli.

Diamanti, I. 2010: Populismo: una definizione indefinita per eccesso di definizioni. *Italianieuropei*, 4. 14 October. Available at: http://www.italianieuropei.it/en/italianieuropei-4-2010/item/1793-populismo-una-definizione-indefinita-per-eccesso-di-definizioni.html[accessed 22 August 2016].

Dominijanni, I. 2013. Quattro punti sul Movimento 5 Stelle. *Il Manifesto*, 15 March.
Eco, U. (1995), *Ur-Fascism*, the New York Review Book,
Eco, U. 2007. *Turning Back the Clock: Hot Wars and Media Populism*. Boston: Houghton Mifflin Harcourt.
The Economist. 2001. *The triumph of populism: How Silvio Berlusconi secured a convincing majority for the centre-right,* 5July. Available at: http://www.economist.com/node/682010 [accessed 15 September 2016].
Eurispes. 2013. *Il Rapporto Italia* 2013 / *L'Italia del presentismo*, 30. January. Available at: http://www.eurispes.eu/content/rapporto-italia-2013-25a-edizione [accessed 17 September 2016].
Eurobarometer. 2012. Available at: http://ec.europa.eu/public_opinion/archives/eb/eb78/eb78_en.htm [accessed 17 September 2016].
Fella, C. and Ruzza, S. 2011. Populism and the Italian right. *Acta Politica*, 46(2), 158–79.
Friedman A. 2015. *My Way. Berlusconi si racconta a Friedman*. Milan: Rizzoli.
Forbes. 2011: *Forbes Silvio Berlusconi profile page*. 11 March. Available at:http://www.forbes.com/profile/silvio-berlusconi/[accessed 11 November 2014].
Gagliardone, I. 2013: A New Italy and the Myth of the Web. *The Huffington Post*, 20 May. Avaiable at: http://www.huffingtonpost.com/iginio-gagliardone/a-new-italy-and-the-myth_b_2906173.html [accessed 14 April 2014].
Gandini, E. 2009. *Videocracy*. Documentary film.
Jones, E. 2007. Party-Based Populism in Europe. *SAIS Review*, XXVII(1), 37–47.
Laclau E. (2007), On Populist Reason, Versobooks, London, New York City
Lanni, A. 2011. *Avanti popoli! Piazze, Tv*, web: *dove va l'Italia senza partiti*. Venezia: Marsilio.
Levin, B. 2002. Cyberhate: A legal and historical analysis of extremist's use of computer networks in America. *American Behavioral Scientist*, 45, 958–88.
Mammone, A., Godin, E. and Jenkins, B. (eds) 2013. Political Science, Varieties of right-wing extremism in Europe. London, New York: Routledge.
Mazzoleni G., Schulz W. (1999), *Mediatization of politics: A Challange for Democracy?*, Political Comunication 16, no.3, 247-261
Mazzoleni, G. 2003. The media and the growth of neo-populism in contemporary democracies. In: The Media and Neo-populism. A Contemporary Comparative Analysis, edited by G. Mazzoleni, J. Stewart and B. Horsefiels. Westpoint, CT: Praeger, 1–20.
Mazzoleni, G., Stewart J. and Horsefield, B. (eds) (2003). *The Media and Neo-populism. A Contemporary Comparative Analysis.* Westport, CT: Praeger.
Mazzoleni, G. 2004. La comunicazione politica. Bologna: il Mulino.
MPM, 2016: *Pluralism and media ownership control.* Available at: http://monitor.cmpf.eui.eu/results-2014/ownership/ [accessed 14 January 2014].
Meny, Y. and Surel, Y. 2002. *Democracies and the populist challenges*. New York: Palgrave MacMillan.
De Montcalon, J.-B., Lemarié, A., d'Allonnes, D.R. and Wieder, T. 2016: Élection présidentielle 2017. *Le Monde.fr*, 1 June. Available at: http://www.lemonde.fr/election-presidentielle-2017/article/2016/06/01/presidentielle-hollande-ne-recueille-que-14-des-intentions-de-vote_4930246_4854003.html [accessed 15 September 2016].
Schafer, J.A. 2002. Spinning the web of hate: web-based hate propagation by extremist organizations. *Journal of Criminal Justice and Popular Culture*, 9(2), 69–88.
Solomon, D. 2007: Questions for Umberto Eco. *Media Studies, The New York Times Magazine*, 25 November. Available at: http://www.nytimes.com/2007/11/25/magazine/25wwln-Q4-t.html?ref=magazine [accessed 12 February 2014].
Study.com. b. d.*What is Representative Democracy? – Definition, Examples, Pros & Cons*. Available at: http://study.com/academy/lesson/what-is-representative-democracy-definition-examples-pros-cons.html [Accessed 23. September 2016].
Taggart, P. 2000. *Populism*. London: Open University Press.
Tronconi, F. (2016), Beppe Grillo's Five Star Movement: Organisation, Communication and Ideology Routledge, 09 mar 2016 - 254 pagine

CYBER SECURITY

NATO Cyber – Challenges & Opportunities

Footnotes
1 G. Alexander Crowther, NATO Nouvelle, Everything Old is New Again. Joint Force Quarterly #78. Fort

McNair, Washington DC. October 2016. Available at http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-83/Article/969675/nato-nouvelle-everything-old-is-new-again/

2 James Stavridis and Elton Parker Sailing the Cyber Sea Joint Force Quarterly #65. Fort McNair, Washington DC. April, 2012. Available at http://www.dtic.mil/docs/citations/ADA595134

3 David Aucsmith, Cyberspace is a Domain of War. May 26, 2010. Available at https://cyberbelli.com/2012/05/26/cyberspace-is-a-domain-of-war/; Martin Libicki, Cyberspace Is Not a Warfighting Domain. I/S: a Journal of Law and Policy for the Information Society. February 2012. Available at http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf

NATO Organization – Civilian Structure. Available at http://www.nato.int/cps/en/natohq/structure.htm

NATO Organization – Military Structure. Available at http://www.nato.int/cps/en/natohq/structure.htm

NATO ACT – Who We Are. Available at http://www.act.nato.int/who-we-are

When referring to NATO documents and doctrine, "defense" is spelled "defence".

All events and dates specified in this paragraph are found at NATO Cyber Defence Evolution. Available at http://www.nato.int/cps/en/natohq/topics_78170.htm#

Where NATO identifies capabilities and promotes their development and acquisition by Allies so that it can meet its security and defense objectives.

NATO Cyber Defence Pledge. Available at http://www.nato.int/cps/en/natohq/official_texts_133177.htm

Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. 6 December 2016. Available at http://www.nato.int/cps/en/natohq/official_texts_138829.htm

NATO. Cyber Defence. Available at http://www.nato.int/cps/en/natohq/topics_78170.htm

Jason Healey, A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.

Real Clear Politics. Significant Cyberattack Incidents. Available at http://www.realclearpolitics.com/lists/cyber_attacks/intro.html

The author has identified the responsible actors based on a variety of sources

James Lewis of the Center for Strategic and International Studies publishes a comprehensive list of cyber attacks, available at https://csis-prod.s3.amazonaws.com/s3fs-public/160824_Significant_Cyber_Events_List.pdf

Allianz Global Corporate & Specialty. A Guide to Cyber Risk. September 2015. Available at http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

Steve Morgan, Forbes. Jan 17 2016. Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Available at https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#1b1d45b13a91

Department of Defense. Joint Publication (JP) 3-12 (R), Cyberspace Operations. 5 February 2013. Page II-4-5

Die Welt. Stoltenberg warns of spike in cyberattacks on NATO Available at http://www.dw.com/en/stoltenberg-warns-of-spike-in-cyberattacks-on-nato/a-37185594

Sky News. Fallon: NATO failing to stop Russian cyber attacks. 17 Feb 2017. Available at http://news.sky.com/story/fallon-nato-failing-to-stop-russian-cyber-attacks-10771630

NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) Crossing the Cyber Rubicon. June 2016. Available at https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf

Deterrence of Cyber-Attacks in International Relations: Denial, Retaliation and Signaling

Footnotes:

[1] Parts of this article have been adapted from: Sico van der Meer, 'Defence, deterrence, and diplomacy. Foreign policy instruments to increase future cyber security', in: Cherian Samuel & Munish Sharma (eds.), S*ecuring cyberspace. International and Asian perspectives,* Pentagon Press, 2016, pp. 95-105.

[2] Virginia Harrison and Jose Pagliery, 'Nearly 1 million new malware threats released every day', CNN Money, 14 April 2015, <http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/>.

[3] International Telecommunication Union, *Trends in Telecommunication Reform 2015*, 2015, p. 4, <www.itu.int/en/publications/Documents/Trends2015-short-version_pass-e374681.pdf>.

[4] Damian Paletta, Danny Yadron, and Jennifer Valentino-Devries, 'Cyberwar Ignites a New Arms Race. Dozens of Countries Amass Cyberweapons, Reconfigure Militaries to Meet Threat', Wall Street Journal, 11 October 2015, <http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128>.

[5] David Elliot, 'Deterring Strategic Cyberattack', *IEEE Security & Privacy*, Vol. 9, 2011, No. 5, p. 38-39.

[6] Neil C. Rowe, 'The attribution of cyber warfare', in: James A. Green (ed.), *Cyber warfare. A multidisciplinary analysis*, Routledge, 2015, pp. 61-72.

[7] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Research Report, RAND Corporation, 2009, p. 65-73.

[8] Ahmer Tarar and Bahar Leventoglu, *Bargaining and Signaling in International Crises*, Research Paper prepared for the United States National Science Foundation, 2008, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.214.823&rep=rep1&type=pdf>.

[9] Sico van der Meer, *Signalling as a foreign policy instrument to deter cyber aggression by state actors*, Clingendael Policy Brief, Netherlands Institute of International Relations 'Clingendael', 2015, <www.clingendael.nl/publication/signaling-foreign-policy-instrument-deter-cyber-aggression>.

[10] Henry Farrell, *Promoting Norms for Cyberspace*, Cyber Brief, Council on Foreign Relations, 2015, <www.cfr.org/cybersecurity/promoting-norms-cyberspace/p36358>.

Toward a Global Norm against Manipulating the Integrity of Financial Data[1]

[1] This article is based on the white paper "Toward a Global Norm Against Manipulating the Integrity of Financial Data" published by the Carnegie Endowment for International Peace on March 27, 2017.

[2] G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015.

[3] G20 Finance Ministers and Central Bank Governors Meeting. G20 Communiqué. Baden-Baden, Germany, 17-18 March 2017.

[4] Krishna N. Das and Jonathan Spicer, "The SWIFT hack - How the New York Fed fumbled over the Bangladesh Bank cyber-heist," Reuters, July 21, 2016, http://www.reuters.com/investigates/special-report/cyber-heist-federal/

[5] Ibid. Section III, Para. 13(f)

[6] States' reliance on financial data and the system's interdependence is likely to increase. For example, in December 2015, The New York Times ran a story about the Swedish government's effort to move the country to an entirely cashless economy and the UN is supporting countries' efforts toward cashless economies through its Better than Cash Alliance. The Indian government is also pursuing a cashless economy.
See Liz Alderman, In Sweden, a Cash-Free Future Nears, N.Y.TIMES (April 26, 2015), http://www.nytimes.com/2015/12/27/business/international/in-sweden-a-cash-free-future-nears.html?_r=0;
BETTER THAN CASH ALLIANCE, https://www.betterthancash.org/ (last visited April 21, 2016).
The Indian Express, "From eradicating black money to cashless economy: PM Modi's changing narrative since demonetisation" December 22, 2016, http://indianexpress.com/article/india/demonetisation-modi-cashless-economy-black-money-narratives-4439843/

[7] John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," The New York Times, August 1, 2009, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html; Richard Clarke and Robert Knake (2010) Cyber War: 202-203

[8] Russia. Draft Convention on International Information Security. 2012. Available online here: http://www.conflictstudies.org.uk/files/20120426_csrc_iisi_commentary.pdf

[9] Mark Fahey & Nicholas Wells, Charts: Who loses when the renminbi joins the IMF basekt?, CNBC (Dec. 2, 2015), http://www.cnbc.com/2015/12/02/who-loses-when-the-renminbi-joins-the-imf-basket.html; Sandhya Dangwal, "Budget 2017: Computer Emergency Response Team to be set up to check cyber frauds," India, February 1, 2017, http://www.india.com/news/india/budget-2017-computer-emergency-response-team-to-be-set-up-to-check-cyber-frauds-1802854/

[10] With regard to counterfeiting currency in wartime, the general counsel of the International Monetary Fund, Francois Gianviti, wrote in a 2004 article, "Does the prohibition against counterfeit currency apply in times of war? There have been instances of such practices." For example, Germany's Operation Bernhard targeted the British economy in World War II. The U.S. government reportedly counterfeited Vietnamese and Iraqi currency during its wars with those countries. F. A. Mann, The Legal Aspect of Money, 5th ed. (Oxford: Oxford University Press, 1992); "Nazi Fake Banknote 'Part of Plan to Ruin British Economy,'" Telegraph, September 29, 2010, http://www.telegraph.co.uk/history/worldwar-two/8029844/Nazi-fake-banknote-part-of-plan-to-ruin-British-economy.html; Lizzie Suiter, Jennifer Hucke, and Courtney Schultz, "The War at Home: A Look at Media Propaganda in WWII, Vietnam, and the War in Iraq" (final paper, Stanford EDGE program, December 2004); Youssef M. Ibrahim, "Fake-Money Flood Is Aimed at Crippling Iraq's Economy," New York Times, May 27, 1992, http://www.nytimes.

com/1992/05/27/world/fake-money-flood-is-aimed-at-crippling-iraq-s-economy.html?pagewanted=all

[11] Nicholas A. Lambert, "The Strategy of Economic Warfare: A Historical Case Study and Possible Analogy to Contemporary Cyber Warfare," in Cyber Analogies, eds. Emily O. Goldman and John Arquilla (Monterey, CA: Naval Postgraduate School, 2014), http://calhoun.nps.edu/bitstream/handle/10945/40037/NPSDA-14-001.pdf?sequence=1

Beyond Ones and Zeroes: Reframing Cyber Conflict

Bibliography:

Giles, Keir, and William Hagestad. 2013. "Divided by a Common Language : Cyber Definitions in Chinese , Russian and English." In *5th International Conference on Cyber Conflict*, 413–29. Tallinn: NATO CCD COE.

Gray, Colin. 2013. "Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling." SSI.

Hare, Forrest. 2012. "The Significance of Attribution to Cyberspace Coercion : A Political Perspective." *4th International Conference on Cyber Conflict*, no. 1966: 125–39.

Healey, Jason. 2016. "Winning and Losing in Cyberspace." In *8th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE.

Iasiello, Emilio. 2013. "Cyber Attack: A Dull Tool to Shape Foreign Policy." In 5*th International Conference on Cyber Conflict,* 451–68. Tallinn: NATO CCD COE.

Jensen, Benjamin M, Brandon Valeriano, and Ryan Maness. 2016. "Cyber Victory : The Efficacy of Cyber Coercion."

Kuehl, Daniel. 2009. "From Cyberspace to Cyberpower: Defining the Problem." In *Cybepower and National Security,* edited by Franklin Kramer, Stuart Starr, and Larry Wentz, 1sted., 24–42. Dulles.

Lawson, Sean. 2013. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology & Politics* 10 (1): 86–103. doi:10.1080/19331681.2012.759059.

Liff, Adam P. 2012. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35 (3): 401–28. doi:10.1080/01402390.2012.663252.

Lindsay, Jon R. 2015. "The Impact of China on Cybersecurity: Fiction and Friction." *International Security* 39 (3): 7–47.

Luiijf, H. A M, Kim Besseling, Maartje Spoelstra, and Patrick de Graaf. 2013. "Ten National Cyber Security Strategies: A Comparison." In *Lecture Notes in Computer Science* (*Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*), 6983 LNCS:1–17. doi:10.1007/978-3-642-41476-3_1.

Maness, Ryan, and Brandon Valeriano. 2015a. "Theories of Cyber Conflict: Restraint, Regionalism, and Cyber Terrorism in the Digital Era." In *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, 45–77. New York, NY: Oxford University Press.

———. 2015b. "The Impact of Cyber Conflict on International Interactions." *Armed Forces & Society*, March, 1–23. doi:10.1177/0095327X15572997.

Nye, By Joseph S. 2010. "Cyber Power," no. May.

Pytlak, Allison, and George F. Mitchell. 2016. "Power, Rivalry and Cyber Conflict: An Emperical Analysis." In *Conflict in Cyber Space*" *Theoretical, Strategic and Legal Perspectives*, edited by Karsten Friis and Jens Ringsmose, 65–82. New York, NY: Routledge.

Rahimi, B. 2003. "Cyberdissent: The Internet in Revolutionary Iran." *Middle East Review of International Affairs* 7 (3): 101–15.

Rivera, Jason. 2015. "Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk." 2015 *7th International Conference on Cyber Conflict*, 7–24.

Ronald Deibert, and Rafal Rohozinski. 2010. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy* 21 (4): 43–57. doi:10.1353/jod.2010.0010.

Shafqat, Narmeen, and Ashraf Masood. 2016. "Comparative Analysis of Various National Cyber Security Strategies." *International Journal of Computer Science and Information Security* (IJSIS) 14 (1): 129–36.

Starr, Stuart. 2009. "Toward a Preliminary Theory of Cyberpower." In *Cyberpower and National Security,* edited by Franklin Kramer, Stuart Starr, and Larry Wentz, 43–88. Washington, D.C.

Valeriano, Brandon, and Ryan Maness. 2013. "A Theory of Cyber Espionage for the Intelligence Community." In *EMC Conference on Intelligence*, National Security, and War. Newport.

Chaos Without Coordination: An Analysis of the EU's Cyber (In)Security

Footnotes:

[1] Cyber attacks are attempts by computer hackers to damage or destroy a computer network or system.

[2] John Leyden, "EU parliament suspends webmail after cyber-attack," The Register, last modified March 31, 2011, http://www.theregister.co.uk/2011/03/31/eu_parliament_hack/.

[3] Ibid. It is estimated that up to 150,000 jobs could be lost in the next few years due to cybercrime.

[4] In this paper, no distinction will be made within the term "cybersecurity." Instead, this paper takes a broad approach to the term and refrains from analyzing specific aspects of the EU's cybersecurity policy, such as cybercrime, cyberwarfare, cyber attacks, or cyber espionage. This is because the EU itself lacks a common definition of such terms. Cybersecurity is thus defined as "the safeguards and actions that can be used to protect the cyber domain … from those threats that are associated with or that may harm its interdependent networks and information structure." See Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final (Feb. 7, 2013).

[5] "A look at Estonia's cyber attack in 2007," NBC News, last modified 2009, http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.WNFYGBjMzyV.

[6] Communication from the Commission to the European Parliament and Council – the EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM (2010) 673 final (Nov. 22, 2010). See also Communication from the Commission to European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Agenda for Europe, COM (2010) 243 final (Aug. 26, 2010).

[7] George Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (Hampshire: Palgrave MacMillan, 2016), 4.

[8] Ibid.

[9] Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review* 56, No. 3 (2011): 571.

[10] Christou, *Cybersecurity in the European Union*, 6.

[11] Ibid., 12. These "conditions" are the circumstances or state of affairs that must exist or be present in a given environment before an effective cybersecurity policy can emerge.

[12] Ibid.

[13] Ibid., 1-9.

[14] Ibid., 27.

[15] Ibid., 29.

[16] Ibid.

[17] While Christou outlines six conditions, this paper focuses on only five of them. The missing condition is the assumption of efficiency abandoned in favour of complexity in governance logics. This condition is not included because due to the capacity of cyber attacks to cause great harm within a short period of time, efficient cybersecurity policies must necessarily act promptly and efficiently to prevent as much damage as possible.

[18] Esther Addley and Josh Halliday, "Operation Payback cripples MasterCard site in revenge from WikiLeaks ban," The Guardian, last modified December 8, 2010, https://www.theguardian.com/media/2010/dec/08/operation-payback-mastercard-website-wikileaks.

[19] Ibid.

[20] Elaine Fahey, "The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security," *European Journal of Risk Regulation* 5, No. 1 (2014): 47. While parties to the Council of Europe Convention on Cybercrime (Budapest Convention) are required to cooperate with such investigations, ratifying the Convention is voluntary and thus not all member states are parties to it.

[21] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012), 66.

[22] Wolfgang Röhrig and Rob Smeaton, "Viewpoints: Cyber Security and Cyber Defence in the European Union,"

European Defence Agency, last modified June 11, 2014, https://www.eda.europa.eu/info-hub/opinion/2014/06/11/viewpoints-cyber-security-and-cyber-defence-in-the-european-union.

[23] RAND Corporation, "Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses" (study commissioned by the European Parliament Committee on Justice, Liberty, and Home Affairs, Brussels, 2015), 107. http://www.rand.org/pubs/research_reports/RR1354.html.

[24] Neil Robinson, "EU cyber-defence: a work in progress," *European Union Institute for Security Studies*, last modified March 14, 2014, http://www.iss.europa.eu/publications/detail/article/eu-cyber-defence-a-work-in-progress/.

[25] Christou, *Cybersecurity in the European Union*, 29.

[26] Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union, COM (2013) 048 final (Feb. 7, 2013).

[27] Directive 2016/1148, of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O. J. (L 194) 1.

[28] RAND Corporation, Cybersecurity in the European Union and Beyond, 50.

[29] Directive 2016/1148, of the European Parliament and of the Council.

[30] Christou, *Cybersecurity in the European Union*, 29.

[31] Directive 2016/1148, of the European Parliament and of the Council.

[32] Ibid.

[33] Ibid.

[34] RAND Corporation, Cybersecurity in the European Union and Beyond, 107.

[35] Scott J. Schackelford and Amanda N. Craig, "Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity," *Stanford Journal of International Law* 50, No. 1 (2014): 119.

[36] Business Software Alliance, "EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace" (study, Washington, 2015), 2. http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf.

[37] Ibid.

[38] Christou, *Cybersecurity in the European Union*, 125.

[39] "NIS Public-Private Platform – Call for expression of interest," European Commission, last modified April 24, 2013, https://ec.europa.eu/digital-single-market/en/news/nis-public-private-platform-—-call-expression-interest.

[40] Christou, *Cybersecurity in the European Union*, 126-127.

[41] Directive 2016/1148, of the European Parliament and of the Council.

[42] Ibid.

[43] Ibid.

[44] RAND Corporation, Cybersecurity in the European Union and Beyond, 16.

[45] Directive 2016/1148, of the European Parliament and of the Council.

[46] Christou, *Cybersecurity in the European Union*, 29.

[47] Petra Vermeulen, "Failed to Connect: An Analysis of European Decisiveness in Cybersecurity Policy" (Master's Thesis, Universiteit Leiden, 2015), 6. https://openaccess.leidenuniv.nl/handle/1887/38208.

[48] Krzysztof Feliks Sliwinski, "Moving beyond the European Union's weakness as a cyber-security agent," *Contemporary Security Policy* 35, No. 3 (2014): 4.

[49] Vermeulen, Failed to Connect, 6.

[50] Eric Kodar, "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I," *ENDC Proceedings* 15 (2012): 107-132.

[51] Vermeulen, Failed to Connect, 6.

[52] Christou, *Cybersecurity in the European Union*, 29.

[53] Thomas Renard, "The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security" (European Strategic Partnerships Observatory Working Paper 7, FRIDE, Edgemont Institute, Brussels and Madrid, 2014), 13. http://www.egmontinstitute.be/wp-content/uploads/2014/06/ESPO-WP7.pdf.

Sliwinski, Moving beyond, 4.

[55] "2014-2017 Cyber Security Strategy," *Estonia Ministry of Economic Affairs and Communications*, last modified 2014, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

[56] Ibid.

[57] "National Cyber Security Strategy 2016 to 2021," GOV.UK, last modified November 1, 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

[58] Ibid.

[59] Emmanuel Darmois, and Geneviève Scméder, "Cybersecurity: A Case for A European Approach" (Paper commissioned by the Human Security Study Group, Security in Transition: An Interdisciplinary Investigation into the Security Gap, London School of Economics and Political Science, London, 2016), 13. http://www.feslondon.org.uk/cms/files/fes/img/publications/FES_LSE_Cybersecurity_Schmeder_Darmois_2016%2002%2023.pdf.

[60] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Cybersecurity Strategy of the European Union.

[61] RAND Corporation, Cybersecurity in the European Union and Beyond, 112.

[62] Sliwinski, Moving beyond, 4.

[63] Christou, *Cybersecurity in the European Union*, 29.

[64] RAND Corporation, Cybersecurity in the European Union and Beyond, 112.

[65] "Cybersecurity." *CENELEC*. Accessed March 20, 2017. https://www.cencenelec.eu/standards/sectors/defencesecurityprivacy/security/pages/cybersecurity.aspx.

[66] Stephanie Simon and Marieke de Goede, "Cybersecurity, Bureaucratic Vitalism and European Emergency," Theory, Culture & Society 32, No. 2 (2015): 93-95.

[67] Communication from the Commission to European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Agenda for Europe.

[68] "European Cybercrime Centre – EC3," Europol, accessed March 5, 2017, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[69] "Cybercrime," *European Commission*, accessed March 6, 2017, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en.

[70] "Capability Development Plan," *European Defence Agency*, accessed March 5, 2017, https://www.eda.europa.eu/what-we-do/eda-priorities/capability-development-plan.

[71] Christou, *Cybersecurity in the European Union*, 2.

[72] Ibid.

[73] "About ENISA," *European Union Agency for Network and Information Security*, accessed March 5, 2017, https://www.enisa.europa.eu/about-enisa.

[74] RAND Corporation, Cybersecurity in the European Union and Beyond, 112.

[75] Darmois and Scméder, Cybersecurity, 14.

[76] European Cyber Security Protection Alliance, "Impact and Contribution Approaches: European Policies and Directives" (working paper, Brussels, 2013), 5. http://www.cspforum.eu/CYSPA_D2_2_1_V2.00.pdf.

[77] RAND Corporation, Cybersecurity in the European Union and Beyond, 57.

Bibliography:

"A look at Estonia's cyber attack in 2007." *NBC News*. Last modified 2009. http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.WNFYGBjMzyV.

"About ENISA." *European Union Agency for Network and Information Security*. Accessed March 5, 2017. https://www.enisa.europa.eu/about-enisa.

Antoni Wierzejski. "Verheugen: EU needs to respond to external, internal chaos." EURACTIV. Last modified July 12, 2013. http://www.euractiv.com/section/global-europe/news/verheugen-eu-needs-to-respond-to-external-internal-chaos/.

Business Software Alliance. "EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace." Study, Washington, 2015. http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf.

"Capability Development Plan." *European Defence Agency*. Accessed March 5, 2017. https://www.eda.europa.eu/what-we-do/eda-priorities/capability-development-plan.

Christou, George. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. Hampshire: Palgrave MacMillan, 2016.

Communication from the Commission to the European Parliament and Council – the EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM (2010) 673 final (Nov. 22, 2010).

Communication from the Commission to European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Agenda for Europe, COM (2010) 243 final (Aug. 26, 2010).

"Cybercrime." *European Commission*. Accessed March 6, 2017. https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en.

"Cybersecurity." *CENELEC*. Accessed March 20, 2017. https://www.cencenelec.eu/standards/sectors/defencesecurityprivacy/security/pages/cybersecurity.aspx.

Darmois, Emmanuel, and Geneviève Scméder. "Cybersecurity: A Case for A European Approach." Paper commissioned by the Human Security Study Group, Security in Transition: An Interdisciplinary Investigation into the Security Gap, London School of Economics and Political Science, London, 2016. http://www.feslondon.org.uk/cms/files/fes/img/publications/FES_LSE_Cybersecurity_Schmeder_Darmois_2016%2002%2023.pdf.

Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press, 2012.

Directive 2016/1148, of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O. J. (L 194) 1.

European Cyber Security Protection Alliance. "Impact and Contribution Approaches: European Policies and Directives," Working Paper, Brussels, 2013. http://www.cspforum.eu/CYSPA_D2_2_1_V2.00.pdf.

"European Cybercrime Centre – EC3." *Europol*. Accessed March 5, 2017. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Esther Addley and Josh Halliday. "Operation Payback cripples MasterCard site in revenge from WikiLeaks ban." *The Guardian*. Last modified December 8, 2010. https://www.theguardian.com/media/2010/dec/08/operation-payback-mastercard-website-wikileaks.

Fahey, Elaine. "The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security." *European Journal of Risk Regulation* 5, No. 1 (2014): 46-60.

John Leyden. "EU parliament suspends webmail after cyber-attack." *The Register*. Last modified March 31, 2011. http://www.theregister.co.uk/2011/03/31/eu_parliament_hack/.

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final (Feb. 7, 2013).

Kodar, Eric. "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I." *ENDC Proceedings* 15 (2012): 107-132.

"National Cyber Security Strategy 2016 to 2021." GOV.UK. Last modified November 1, 2016. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

Neelie Kroes. "Towards a coherent international cyberspace policy for the EU." *European Commission*. Last modified 30 January 2013. http://europa.eu/rapid/press-release_SPEECH-13-82_en.htm?locale=en.

Neil Robinson. "EU cyber-defence: a work in progress." *European Union Institute for Security Studies*. Last modified March 14, 2014. http://www.iss.europa.eu/publications/detail/article/eu-cyber-defence-a-work-in-progress/.

"NIS Public-Private Platform – Call for expression of interest." *European Commission*. Last modified April 24, 2013. https://ec.europa.eu/digital-single-market/en/news/nis-public-private-platform-—-call-expression-interest.

Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union, COM (2013) 048 final (Feb. 7, 2013).

RAND Corporation. "Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses." Study Commissioned by the European Parliament Committee on Justice, Liberty, and Home Affairs, Brussels, 2015. http://www.rand.org/pubs/research_reports/RR1354.html.

Renard, Thomas. "The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security." European Strategic Partnerships Observatory Working Paper 7, FRIDE, Edgemont Institute, Brussels and Madrid, 2014. http://www.egmontinstitute.be/wp-content/uploads/2014/06/ESPO-WP7.pdf.

Schackelford, Scott J., and Amanda N. Craig. "Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity." *Stanford Journal of International Law* 50, No. 1 (2014): 119.

Schmitt, Michael N. "Cyber Operations and the Jus Ad Bellum Revisited." *Villanova Law Review* 56, No. 3 (2011):

569-606.
Simon, Stephanie, and Marieke de Goede. “Cybersecurity, Bureaucratic Vitalism and European Emergency.” *Theory, Culture & Society* 32, No. 2 (2015): 79-106.
Sliwinski, Krzysztof Feliks. “Moving beyond the European Union’s weakness as a cyber-security agent.” *Contemporary Security Policy* 35, No. 3 (2014): 468-486.
Vermeulen, Petra. “Failed to Connect: An Analysis of European Decisiveness in Cybersecurity Policy.” Master’s Thesis, Universiteit Leiden, 2015. https://openaccess.leidenuniv.nl/handle/1887/38208.
Wolfgang Röhrig and Rob Smeaton. “Viewpoints: Cyber Security and Cyber Defence in the European Union.” *European Defence Agency*. Last modified June 11, 2014. https://www.eda.europa.eu/info-hub/opinion/2014/06/11/viewpoints-cyber-security-and-cyber-defence-in-the-european-union.
“2014-2017 Cyber Security Strategy.” *Estonia Ministry of Economic Affairs and Communications*. Last modified 2014. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

The Thin Line Between Utopia and Dystopia: policing child porn on the Darknet

Footnotes:

[1] To better understand the differences one should look at the Deep Web in the image of subterranean mining. If anything above ground is part of the “searchable Internet,” then anything below it is part of the Deep Web—inherently hidden, harder to get to, and not readily visible. The Dark Web would be the deeper portion of the Deep Web that requires highly specialized tools or equipment to access. It lies deeper underground and site owners have more reason to keep their content hidden (Ciancaglini, 5)

[2] Particularly, dynamic web pages, blocked sites, unlinked sites, private sites, non-HTML/Contextual/ Scripted Content, Limited-access networks

[3] To give an idea, according to the FBI, during the two-and-a-half years of existence, the Silk Road, with over a million transactions, alone generated $120 Billion in sales and $80 million in commission (Balduzzi 11). A congressional report estimated the annual cost of cybercrime to adults in 24 countries across the globe at $113 billion (Finale 1).

[4] People who are concerned about political or economic retribution, harassment or even threats to their lives, use .onion routing to ramp up their personal security when surfing the web.

[5] Most notably companies like Facebook, The New Yorker, DuckDuckGo have set up “.onion” Dark Websites, accessible through Tor browser.

[6] At least 750 TB of data, roughly forty times the size of the known surface web, with over 85 billion records or documents (Bergman 21).

[7] Especially remembering the size of the Dark Web and unfamiliar methods to monitor it. In addition, the naming and address schemes in the Deep Web often change. This means that the information we harvested two weeks ago is no longer relevant today. This also unfortunately has implications in proving crime.

[8] Among many other strange communities: social media racists, cam girls, self-harm communities, crypto-anarchists and transhumanists (Biyrukov 186)

[9] Category A includes rape or sexual torture of children

[10] For example, in October 2011 the “hacktivist” collective Anonymous, through its Operation Darknet, crashed a website hosting service called Freedom Hosting—operating on the Tor network—which was reportedly home to more than 40 child pornography websites. Among these websites was Lolita City, cited as one of the largest child pornography sites with over 100GB of data. Anonymous had “matched the digital fingerprints of links to Freedom Hosting” and then launched a Distributed Denial of Service (DDoS) attack against Freedom Hosting. In addition they leaked the user database—including username, membership time, and number of images uploaded—for over 1,500 Lolita City members (Finklea 8).

[11] At its peak, Playpen, the largest Darknet CP site, had almost 215,000 members. It had more than 117,000 posts and received an average of 11,000 unique visitors a week and discovered numerous posts featuring extreme child abuse imagery, as well as providing advice on how potential child sex abusers could avoid detection online (Russon).

[12] Avoiding negative outcomes of policing and other ostensibly prevention-oriented practices and preserving investigative resources for only the most concerning cases.

Bibliography:

Ablon, Lillian, and Martin Libicki. "Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data." *Defense Counsel Journal* 82.2 (2015): 143-52. *JSTOR [JSTOR]*. Web. 5 Nov. 2016.

Acquisti, Alessandro, Roger DIngledine, and Paul Syverson. *On the Economics of Anonymity*. Berkeley. ONR, 2002. Web. 4 Nov. 2016.

Adar, Eytan, and Bernardo A. Huber. "Free Riding on Gnutella." *First Monday* 5.10 (2000): 1-11. *JSTOR*. Web. 15 Nov. 2016.

Aldridge, Judith. *Not an 'eBay for Drugs': The Cryptomarket "Silk Road" As a Paradigm Shifting Criminal Innovation. SSRN*. University of Manchester, University of Lausanne, 3 July 2014. Web. 3 Nov. 2016.

Allison, Ian. "Bitcoin Tumbler: The Business of Covering Tracks in the World of Cryptocurrency Laundering." *International Business Times UK. IBTimes*, 13 Feb. 2015. Web. 22 Nov. 2016.

Arohl, Te. "How to Navigate the Deep Web | Features | Critic.co.nz." *The Critic*. Ed. Zane Pocock. Planet Media, 23 Nov. 2016. Web. 22 Nov. 2016.

Bancroft, Angus, and Peter Scott Reid. "Challenging the Techno-politics of Anonymity: The Case of Cryptomarket Users." *Information, Communication & Society* (2016): 1-16. JSTOR [JSTOR]. Web. 5 Nov. 2016.

Bancroft, Angus, and Peter Scott Reid. "Concepts of Illicit Drug Quality among Darknet Market Users: Purity, Embodied Experience, Craft and Chemical Knowledge." *International Journal of Drug Policy* 35 (2016): 42-49. *JSTOR [JSTOR]*. Web. 4 Oct. 2016.

Barbosa, Luciano, and Juliana Freire. *An Adaptive Crawler for Locating Hidden-Web Entry Points*. University of Utah. International World Wide Web Conference, 8 May 2007. Web. Oct. 2016.

Beckett, Andy. "The Dark Side of the Internet." *The Guardian*. Guardian News and Media, 25 Nov. 2009. Web. 20 Nov. 2016. <https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet>.

Bergman, Michael. *The Deep Web: Surfacing Hidden Value. Deep Content*. Brightcove, 24 Sept. 2001. Web. 19 Nov. 2016.

Bharara, Preet. "Cyber Security: Protecting Our Cyber Citizens." *Advances in Cyber Security: Technology, Operations, and Experiences*. Ed. D. Frank Hsu and Dorothy Marinucci. New York: Fordham UP, 2013. N. pag. Print.

Biddle, Peter, Paul England, Marcus Peinado, and Bryan Willman. *The Darknet and the Future of Content Distribution*. Stanford University. Microsoft Corporation, 2003. Web. Nov. 2016.

Biryukov, Alex, Ivan Pustogarov, and Ralf-Phillipp Weinmann. *Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization. 2013 IEEE Symposium on Security and Privacy*. University of Luxembourg, 2013. Web. 4 Oct. 2016.

Brightplan Staff. "Clearing Up Confusion - Deep Web vs. Dark Web." *BrightPlanet*. Brightplanet, 10 May 2016. Web. 20 Nov. 2016. <https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/>.

Brightplanet WebCollection. "Deep Web: A Primer - BrightPlanet." BrightPlanet. *BrightPlanet* WebCollection, 10 May 2016. Web. 20 Nov. 2016.

Broadhurst, Roderic, and Peter Grabosky. "The Global Cyber-Crime Problem: The Socio-Economic Impact." *Cyber-Crime: The Challenge in Asia*. By Peter Grabosky. N.p.: Hong Kong UP, 2005. N. pag. Print.

Bryant, Bill. "*Designing an Authentication System: A Dialogue in Four Scenes*." Designing an Authentication System: A Dialogue in Four Scenes. MIT, 1997. Web. 24 Nov. 2016.

Buchanan, Ben. "Cryptography and Sovereignty." *Survival* 58.5 (2016): 95-122. JSTOR [JSTOR]. Web. 7 Mar. 2016.

Buchanan, Ben. "The Life Cycles of Cyber Threats." *Survival* 58.1 (2016): 39-58. JSTOR [JSTOR]. Web. 4 Oct. 2016.

Burrell, Ian. "The Dark Net:Inside the Digital Underworld by Jamie Bartlett, Book Review." *The Independent*. Independent Digital News and Media, 28 Aug. 2014. Web. 20 Nov. 2016.

Buxton, Julia, and Tim Bingham. *The Rise and Challenge of Dark Net Drug Markets. Policy Brief/Swansea University*. Global Drug Policy Observatory, 7 Jan. 2015. Web. 3 Nov. 2016.

Chacos, Brad. "Meet Darknet, the Hidden, Anonymous Underbelly of the Searchable Web." *PCWorld*. PCWorld, 12 Aug. 2013. Web. 20 Nov. 2016.

Chen, Adrian. "The Underground Website Where You Can Buy Any Drug Imaginable." *Gawker*. Gawker, 1 Nov. 2011. Web. 20 Nov. 2016.

Chertoff, Michael, and Toby Simon. *The Impact of the Dark Web on Internet Governance and Cyber Security. Paper Series: No 6*. Chatham House, 5 Feb. 2015. Web. 10 Nov. 2016.

Ciancaglini, Vincenzo, Marco Balduzzi, Max Goncharov, Robert McArdle, and Forward-Looking Threat Research Team. *Deepweb and Cybercrime It's Not All About TOR. Micro Research Paper*. Trend Micro, 2013. Web. 5 Nov. 2016.

Ciancaglini, Vincenzo, Marco Balduzzi, Robert McArdle, and Forward-Looking Threat Research Team. *Below The Surface: Exploring the Deep Web. Trendlabs Research Paper*. Trend Micro, 2015. Web. 13 Nov. 2016.

Cox, Christopher. "Cyber Capabilities and Intent of Terrorist Forces." *Information Security Journal: A Global Perspective* 24.1-3 (2015): 31-38. JSTOR [JSTOR]. Web. 5 Nov. 2016.

Cox, Joe. "A Dark Web Hacker Is Hunting Potential Pedophiles to Extort Them for Money." *Motherboard*. Vice, 12

Nov. 2015. Web. 20 Nov. 2016.

Cox, Joeseph. "The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers." *Motherboard*. Vice, 5 Jan. 2016. Web. 19 Nov. 2016.

Cox, Joseph. "Dark Web Vendor Sentenced for Dealing Counterfeit Coupons." *Motherboard*. Vice, 14 Jan. 2016. Web. 20 Nov. 2016.

Cox, Joseph. "This Fake Hitman Site Is the Most Elaborate, Twisted Dark Web Scam Yet." *Motherboard*. Vice, 14 Jan. 2016. Web. 20 Nov. 2016.

Cox, Joseph. "The UK Will Police the Dark Web with a New Task Force." *Motherboard*. Vice, 8 Nov. 2015. Web. 20 Nov. 2016.

Cox, Joseph. "What Firewall? China's Fledgling Deep Web Community." *Motherboard*. Vice, 25 Feb. 2015. Web. 20 Nov. 2016.

Cuthberson, Anthony. "'Calm down Isis': Hackers Hit Islamic State Propaganda Site on the Dark Web with an Advert for Prozac." *International Business Times* UK. IBTIMES UK, 25 Nov. 2015. Web. 20 Nov. 2016.

David Rose for The Mail on Sunday. "Secrets of the UK's New FBI: Police Chief Reveals Elite Force of 5,000 'super' Agents Will Wage a High-tech Manhunt for Britain's Most Wanted Criminals." *Mail Online*. Associated Newspapers, 06 Oct. 2013. Web. 20 Nov. 2016.

Deep Web. Dir. Alex Winter. Perf. Keanu Reeves. *Deep Web*. Epix, 9 Aug. 2015. Web. 4 Oct. 2016.

Dingledine, Roger, Nick Mathewson, and Paul Syverson. *Tor: The Second-Generation Onion Router. Tor Design*. ONR and DARPA, 2004. Web. 5 Oct. 2016.

Drucker, Susan J., and Gary Gumpert. "Cybercrime and Punishment." *Critical Studies in Media Communication 17.2* (2000): 133-58. *JSTOR [JSTOR]*. Web. 3 Nov. 2016.

Duffin, Tony. "Opinion: A New Drug Trade Is Hiding in the Underbelly of the Internet." *TheJournal.ie*. Prass Association, 14 Mar. 2014. Web. 23 Nov. 2016.

Editors on Deep Dot Web. "Beware of Phishing Scams On Clearnet Sites! (darknetmarkets.org)." *Deep Dot Web*. Deep Dot Web, 05 July 2015. Web. 19 Nov. 2016.

Editors. "Warning: More Onion Cloner Phishing Scams." *Deep Dot Web*. Deep Dot Web, 22 Apr. 2015. Web. 19 Nov. 2016.

Egan, Matt. "What Is the Dark Web? How to Access the Dark Web. What's the Difference between the Dark Web and the Deep Web?" PC Advisor. *PCAdvisor*, 28 Apr. 2016. Web. 20 Nov. 2016.

Evans, Robert, Douglas A. McDonnell, Alex Race, Ian Ury, C.K.Bond, Codie Martin, Doron S., Luke T. Harrington, Cole Gamble, and Diana McCallum. "5 Things I Learned Infiltrating Deep Web Child Molesters." *Cracked.com*. Cracked, 16 June 2016. Web. 19 Nov. 2016.

FedEx. "FedEx Faces More Charges over Shipping of Illegal Prescription Drugs." *Post Parcel RSS. Triangle*, 8 Aug. 2014. Web. 23 Nov. 2016.

Finale, Kristin. *Dark Web. Congressional Research Brief*. Congressional Research Service, 7 July 2015. Web. 15 Nov. 2016.

Franceschi-Bicchieral, Lorenzo. "Hackers Tried To Hold a Darknet Market For a Bitcoin Ransom." *Motherboard*. Vice, 13 May 2016. Web. 20 Nov. 2016.

Franklin-Wallis, Oliver. "Unravelling the Dark Web." *British GQ*. GQ, 7 Feb. 2013. Web. 21 Nov. 2016.

Garcia, Frank. "Business and Marketing on the Internet." *Business and Marketing on the Internet*. WaybackMachine, Jan. 1996. Web. 20 Nov. 2016. <https://web.archive.org/web/19961205083117/http://tcp.ca/Jan96/BusandMark.html>.

Ghappour, Ahmed. "Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance." *Just Security*. NYU Law, 30 Apr. 2016. Web. 19 Nov. 2016.

Glenny, Misha. *DarkMarket: Cyberthieves, Cybercops, and You*. New York, NY: Alfred A. Knopf, 2011. Print.

Glenny, Misha. *McMafia: A Journey through the Global Criminal Underworld*. New York: Knopf, 2008. Print.

Goldschlag, David M Reed,Michael G. & Syverson, Paul F 'Hiding *Routing Information, Workshop on Information Hiding*, Cambridge, UK, 1996.

Golle, Phillippe, Kevin Leyton-Brown, Ilya Mironov, and Mark Lillibridge. "*Incentives for Sharing in Peer-to-Peer Networks*." Electronic Commerce WELCOM (2001): 75-89. *Jstor*. Web. 13 Oct. 2016.

Greenberg, Andy. "Hacker Lexicon: What Is the Dark Web?" *Wired.com*. Conde Nast Digital, 19 Nov. 2014. Web. 20 Nov. 2016. <https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>.

Greenberg, Andy. "An Interview With Darkside, Russia's Favorite Dark Web Drug Lord." *Wired.com*. Conde Nast Digital, 4 Dec. 2015. Web. 21 Nov. 2016.

Greenberg, Andy. "Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds." *Wired*. Wired, 12 Jan. 2014. Web. 10 Oct. 2016.

Haetala, Laura. "How Bin Laden Evaded the NSA: Sneakernet." *CNET*. CNET, 13 May 2011. Web. 21 Nov. 2016.

Hargreaves, Susle. *Annual Report 2015. Annual Report 2015. Internet Watch Foundation, 2015*. Web. 5 Oct. 2016.

Hawkins, Brett. *Under The Ocean of the Internet - The Deep Web*. InfoSec Reading Room. Sans Institute, 15 May 2016. Web. 4 Nov. 2016.

He, Bin, Mitesh Patel, Zen Zhang, and Kevin Chen-Chuan Chang. *ACCESSING THE DEEP WEB. Communications of the ACM*. ACM, May 2007, Nov 2016.

Holt, Thomas J. "Exploring the Intersections of Technology, Crime, and Terror." *Terrorism and Political Violence* 24.2 (2012): 337-54. *JSTOR [JSTOR]*. Web. 23 Nov. 2016.

Hughes, Eric. "A Cypherpunk's Manifesto." *A Cypherpunk's Manifesto*. N.p., n.d. Web. 24 Nov. 2016.

InfoSec EXPLOIT DEVELOPMENT. "Cyber Criminal Ecosystems in the Deep Web." *InfoSec Resources Cyber Criminal Ecosystems in the Deep Web Comments*. InfoSec, 22 Mar. 2016. Web. 01 Dec. 2016.

ITA. *US Subcommittee Public Awareness Task Force*. Publication no. Anticounterfeiting on the Dark Web. International Trademark Association, 13 Apr. 2015. Web. 21 Nov. 2015.

Jenkins, Philip. *Beyond Tolerance: Child Pornography on the Internet*. New York: New York UP, 2001. Print.

Koebler, Jason. "The Closest Thing to a Map of the Dark Net: Pastebin." *Motherboard*. Vice, 23 Feb. 2015. Web. 20 Nov. 2016.

Koebler, Jason. "Six Ways Law Enforcement Monitors the Dark Web." *Motherboard*. Vice, 17 Feb. 2015. Web. 20 Nov. 2016.

Kushner, David. "The Autistic Hacker." *IEEE Spectrum: Technology, Engineering, and Science News*. IEEE, 27 June 2011. Web. 20 Nov. 2016.

Lachow, Irving. "Cyber Terrorism: Menace or Myth?" *Cyberpower and National Security*. By Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, D.C: Center for Technology and National Security Policy, 2009. N. pag. Print.

Langewiesche, William. "Welcome to the Dark Net, a Wilderness Where Invisible World Wars Are Fought and Hackers Roam Free." The Hive. Vanity Fair, 11 Sept. 2016. Web. 20 Nov. 2016.

Levine, Yashi. "Almost Everyone Involved in Developing Tor Was (or Is) Funded by the US Government." *Pando*. Pandomedia, 16 July 2014. Web. 19 Nov. 2016.

Lim, Kevjn. "Big Data and Strategic Intelligence." *Intelligence and National Security* 31.4 (2015): 619-35. *JSTOR [JSTOR]*. Web. 5 Oct. 2016.

Lusthaus, Jonathan. "How Organised Is Organised Cybercrime?" *Global Crime* 14.1 (2013): 52-60. *JSTOR [JSTOR]*. Web. 23 Nov. 2016.

Lusthaus, Jonathan. "Trust in the World of Cybercrime." *Global Crime* 13.2 (2012): 71-94. *JSTOR [JSTOR]*. Web. 3 Nov. 2016.

Maddox, Alexia, Monica J. Barratt, Matthew Allen, and Simon Lenton. "Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital â˜demimondeâ™." *Information, Communication & Society* 19.1 (2015): 111-26. JSTOR [JSTOR]. Web. 5 Nov. 2016.

May, Timothy M. "Crypto Anarchy and Virtual Communities." *Crypto Anarchy and Virtual Communities*. Cypherpunks Group, July 1988. Web. 23 Nov. 2016. distributed on the Usenet and on various mailing lists.

McCusker, Rob. "Transnational Organised Cyber Crime: Distinguishing Threat from Reality." *Crime Law Soc Change* 46 (2007): 257-73. Jstor. Web. 10 Oct. 2016.

McMillan, Robert. "FBI: Cybercriminals Taking Cues From Mafia." *PC World*. IDG News Service, 07 Aug. 2006. Web. 17 Nov. 2016.

Mitnick, Kevin D., and William L. Simon. *Ghost in the Wires: My Adventures as the World's Most Wanted* Hacker. New York: Little, Brown, 2011. Print.

Moore, Daniel, and Thomas Rid. "Cryptopolitik and the Darknet." *Survival* 58.1 (2016): 7-38. *JSTOR [JSTOR]*. Web. 5 Nov. 2016.

News, BBC. "Jihadist Cell in Europe 'sought Recruits for Iraq and Syria'" *BBC News*. BBC., 12 Dec. 2015 Web. 20 Nov. 2016.

O'Brien, Mark. "The Internet, Child Pornography and Cloud Computing: The Dark Side of the Web?" *Information & Communications Technology Law* 23.3 (2014): 238-55. JSTOR [JSTOR]. Web. 4 Nov. 2016.

Ormsby, Eileen. "The New Underbelly." *The Age*. The Age Australia, 31 May 2012. Web. 20 Nov. 2016.

Owen, Gareth, and Nick Savage. "The Tor Dark Net." *Global Commission on Internet Governance* 20th ser. September (2015): 1-20. JSTOR [JSTOR]. Web. 4 Oct. 2016.

Paganini, Pierluigi. "Project Artemis – OSINT Activities on Deep Web." *InfoSec Resources Project Artemis OSINT Activities on Deep Web Comments*. Infosec Institute, 1 July 2013. Web. 21 Nov. 2016.

Paganini, Pierluigi. "What Is the Deep Web? A First Trip into the Abyss." *Security Affairs*. Security Affairs, 30 Apr.

2013. Web. 21 Nov. 2016.
Paul, Kari. "Coming Soon to the Deep Web: Adorable Baked Goods." *Motherboard*. Vice, 20 Sept. 2015. Web. 20 Nov. 2016.
Reeve, Tom. "Extortion on the Cards." *SC Magazine UK*. SC UK, 23 Sept. 2015. Web. 20 Nov. 2016.
Rich, Steven, Craig Timberg, and Barton Gellman. "Secret NSA Documents Show Campaign against Tor Encrypted Network." Washington Post. *The Washington Post*, 4 Oct. 2013. Web. 20 Nov. 2016.
Richet, Jean-Loup. *Laundering Money Online: A Review of Cybercriminals' Methods. Tools and Resources for Anti-Corruption Knowledge*. United Nations Office on Drugs and Crime, 1 June 2013. Web. 4 Nov. 2016.
Robertson, Adi. "New Report Says the NSA Is Checking Who Visits Tor&#39;s Website." *The Verge*. The Verge, 03 July 2014. Web. 20 Nov. 2016.
Robertson, Adi. "NSA Tried and Failed to Compromise Tor, but Browser Vulnerabilities Gave Some Users Away." *The Verge*. The Verge, 04 Oct. 2013. Web. 20 Nov. 2016.
Russon, Mary-Ann. "FBI Crack Tor and Catch 1,500 Visitors to Biggest Child Pornography Website on the Dark Web." *International Business Times UK*. IBT, 07 Jan. 2016. Web. 02 Dec. 2016.
Sandywell, Barry. "Monsters in Cyberspace Cyberphobia and Cultural Panic in the Information Age." *Information, Communication & Society* 9.1 (2006): 39-61. *JSTOR [JSTOR]*. Web. 23 Nov. 2016.
Saroiu, Stefan, Krishna P. Gummadi, and Steven D. Gribble. *A Measurement Study of Peer-to-Peer File Sharing Systems. Washington University*. University of Washington Computing and Communications Services and the Department of Computer Science and Engineering, 2001. Web. 14 Nov. 2016.
Schmidt, Howard. "Cyber Security: Securing Our Cyber Ecosystem." *Advances in Cyber Security: Technology, Operations, and Experiences*. By D. Frank Hsu and Dorothy Marinucci. New York: Fordham UP, 2013. N. pag. Print.
Schwartz, Mattathias. "The Trolls Among Us." The New York Times. The New York Times, 02 Aug. 2008. Web. 22 Nov. 2016.
Seddon, Toby. "Drug Policy and Global Regulatory Capitalism: The Case of New Psychoactive Substances (NPS)." *International Journal of Drug Policy* 25.5 (2014): 1019-024. *JSTOR [JSTOR]*. Web. 4 Nov. 2016.
Senker, Cath. *Cybercrime & the Dark Net*. N.p.: Sirius, 2016. Print.
Shannon, Julie, and Nick Thomas. "Human Security and Cyber-Security: Operationalising a Policy Framework." *Cyber-crime: The Challenge in Asia*. Ed. Roderic Broadhurst and Peter Grabosky. N.p.: Hong Kong UP., 2005. N. pag. Jstor. Web. 18 Nov. 2016.
Shostack, Adam, and Paul Syverson. *WHAT PRICE PRIVACY? 2nd Annual Workshop on Economics and Information Security,* College. N.p., May 2003. Web. 4 Nov. 2016.
Sigaint. "Interview With "Sigaint DarkNet Email" Admin." *Deep Dot Web*. Deep Dot Web, 16 Feb. 2015. Web. 20 Nov. 2016.
Simonite, Tom. ""Dark Web" Version of Facebook Shows a New Way to Secure the Web." *MIT Technology Review*. MIT, 3 Nov. 2013. Web. 4 Oct. 2016.
Simonite, Tom. "The Surprising Light Side of the Dark Web." *MIT Technology Review*. MIT, 18 Mar. 2016. Web. 20 Nov. 2016.
Singer, Peter W. "The Cyber Terror Bogeyman." *Brookings*. Brookings Institute, 31 Oct. 2012. Web. 22 Nov. 2016.
Smallbone, Stephen, PH.D. *Queensland Child Protection Commission of Inquiry*. 2012. Expert Statement. Griffith University, Queensland.
Solon, Olivia. "Police Crack down on Silk Road following First Drug Dealer Conviction." *Ars Technica*. Wired.uk, 03 Feb. 2013. Web. 20 Nov. 2016.
Suler, John. "The Online Disinhibition Effect." *CyberPsychology & Behavior* 7.3 (2004): 321-26. JSTOR [JSTOR]. Web. 3 Nov. 2016.
Staff, Ars. "Feds Bust through Huge Tor-hidden Child Porn Site Using Questionable Malware." *Ars Technica*. Ars Technica, 16 July 2015. Web. 19 Nov. 2016.
Stockley, Mark. "Can You Trust Tor's Exit Nodes?" Naked Security. Sophos, 26 June 2015. Web. 19 Nov. 2016.
Stockley, Mark. "The Dark Web: Anarchy, Law, Freedom and Anonymity." Naked Security. Sophos, 20 Feb. 2015. Web. 19 Nov. 2016.
Stockley, Mark. "Hundreds of Dark Web Sites Cloned and "booby Trapped"." *Naked Security*. Sophos, 31 Dec. 2015. Web. 19 Nov. 2016.
Stockley, Mark. "Is DARPA's Memex Search Engine a Google-killer?" *Naked Security*. Sophos, 14 Apr. 2015. Web. 02 Dec. 2016.
Swartz, Aaron. "In Defense of Anonymity." *Raw Thought*. Aaron Swartz, n.d. Web. 20 Nov. 2016.
Syverson, Paul. *The Paradoxical Value of Privacy*. Naval Research Laboratory. Naval Research Laboratory, 14 Mar. 2003. Web. 3 Nov. 2016.

Tucker, Patrick. "If You Do This, the NSA Will Spy on You." *Defense One*. Defense One, 7 July 2014. Web. 21 Nov. 2016.

Viney, Steven. "Explainer: What Is the Dark Net?" *ABC News*. Australian Broadcast Channel, 27 Jan. 2016. Web. 20 Nov. 2016.

Wall*, David S. "Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime1." *International Review of Law, Computers & Technology* 22.1-2 (2008): 45-63. *JSTOR [JSTOR]*. Web. 3 Nov. 2016.

Ward, Mark. "Tor's Most Visited Hidden Sites Host Child Abuse Images." *BBC News*. BBC, 30 Dec. 2014. Web. 20 Nov. 2016.

Weimann, Gabriel. "Going Dark: Terrorism on the Dark Web." *Studies in Conflict & Terrorism* 39.3 (2015): 195-206. *JSTOR [JSTOR]*. Web. 4 Nov. 2016.

Whoriskey, Peter. "Firms Push for a More Searchable Federal Web." *Washington Post*. The Washington Post, 11 Dec. 2008. Web. 20 Nov. 2016.

Wiener-Bronner, Danielle. "NASA Is Indexing the 'Deep Web' to Show Mankind What Google Won't." *Fusion*. Fusion Media, 6 Oct. 2015. Web. 20 Nov. 2016. <http://fusion.net/story/145885/nasa-is-indexing-the-deep-web-to-show-mankind-what-google-wont/>.

Willacy, Mark. "Detectives Took on Paedophile's Identity in 'dark Net' Abuse Sting." *ABC News*. Australia Broadcast Network, 26 Aug. 2015. Web. 20 Nov. 2016.

Wilson, Clay. "Cyber Crime." *Cyberpower and National Security*. By Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, D.C: Center for Technology and National Security Policy, 2009. N. pag. Print.

Wright, Alex. "Exploring a 'Deep Web' That Google Can't Grasp." *The New York Times*. The New York Times, 22 Feb. 2009. Web. 20 Nov. 2016. <http://www.nytimes.com/2009/02/23/technology/internet/23search.html?th&emc=th&mtrref=undefined>.

Zetter, Kim. "Going Dark: The Internet Behind The Internet." *NPR*. NPR, 25 May 2014. Web. 20 Nov. 2016. <http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet>.

Zetter, Kim. "Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise." *Wired*. Conde Nast Digital, 9 Oct. 2007. Web. 19 Nov. 2016.

Zetter, Kim. "Tor Torches Online Tracking." *Wired.com*. Conde Nast Digital, 17 Jan. 2005. Web. 19 Nov. 2016.

Zetter, Kim. "Darpa Is Developing a Search Engine for the Dark Web." *Wired*. Conde Nast, 10 Dec. 2015. Web. 02 Oct. 2016.

In this issue:

Populism in the Digital Age

Cyber Security

International Affairs Forum

www.ia-forum.org