68

AICGSPOLICYREPORT

MOVING BEYOND CYBER WARS: A TRANSATLANTIC DIALOGUE

Karsten Geier
Inger-Luise Heilmann
Jackson Janes
Kent Logsdon
Gregor Kutzschbach
Sarah Lohmann
Reinhard Meier-Walser
Andreas Nick
Andrea Rotter
Maximilian Rückert
Bret Schafer
Matthias Schulze
Scott W. Tousley

AMERICAN INSTITUTE FOR CONTEMPORARY GERMAN STUDIES THE JOHNS HOPKINS UNIVERSITY

American Institute
for Contemporary
German Studies

JOHNS HOPKINS UNIVERSITY

35 YEARS
BUILDING A SMARTER
PARTNERSHIP

The American Institute for Contemporary German Studies strengthens the German-American relationship in an evolving Europe and changing world. The Institute produces objective and original analyses of developments and trends in Germany, Europe, and the United States; creates new transatlantic networks; and facilitates dialogue among the business, political, and academic communities to manage differences and define and promote common interests.

ISBN 978-1-933942-64-3

ADDITIONAL COPIES:
Additional Copies of this Policy Report are available for $10.00 to cover postage and handling from the American Institute for Contemporary German Studies, 1755 Massachusetts Avenue, NW, Suite 700, Washington, DC 20036. Tel: 202/332-9312, E-mail: info@aicgs.org Please consult our website for a list of online publications: http://www.aicgs.org

The views expressed in this publication are those of the author(s) alone. They do not necessarily reflect the views of the American Institute for Contemporary German Studies.

Hanns
Seidel
Stiftung

This publication was produced in cooperation with the Hanns-Seidel-Stiftung.

Additional support was provided by the AICGS Foreign & Domestic Policy Program.

Table of Contents

ABOUT THE AUTHORS

Karsten Geier is the head of the German diplomatic mission in Mazar-e-Sharif. During the Transatlantic Cybersecurity Partnership, he was head of the Cyber Policy Coordination Staff in Germany's Federal Foreign Office. A career Foreign Service officer, Mr. Geier has held a variety of posts both at home and abroad. He has served in Southeastern Europe, in Brussels at Germany's Representation to the European Union, and in Washington, DC, including as exchange officer in the U.S. Department of State. His most recent assignment abroad led him to New York, where he helped set up the European Union Delegation and subsequently worked at Germany's Mission to the United Nations. Mr. Geier was Germany's member of the 2014/2015 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and chaired the 2016/2017 Group. A frequent public speaker and author of articles on international cyber affairs, Mr. Geier has also taught modules or given presentations at Germany's Federal Academy for Security Policy, the Foreign Service Academy, the Führungsakademie der Bundeswehr (German Armed Forces' Leadership College), the European Security and Defense College, the George C. Marshall Center, and other educational institutions.

Inger-Luise Heilmann is a parliamentary advisor to Dr. Andreas Nick, member of the German Bundestag. Her field of work includes the preparation of the deputy's work in the Foreign Affairs Committee and the Committee on Digitalization as well as the Subcommittee on United Nations, International Organizations and Globalization. She holds a Master's Degree in International Relations with a Specialization on Security from Rijksuniversiteit Groningen.

Jackson Janes is the President Emeritus of the American Institute for Contemporary German Studies at the Johns Hopkins University in Washington, DC, where he has been affiliated since 1989. Dr. Janes has been engaged in German-American affairs in numerous capacities over many years. He has studied and taught in German universities in Freiburg, Giessen and Tübingen. He was the Director of the German-American Institute in Tübingen (1977-1980) and then directed the European office of The German Marshall Fund of the United States in Bonn (1980-1985). Before joining AICGS, he served as Director of Program Development at the University Center for International Studies at the University of Pittsburgh (1986-1988). He was also Chair of the German Speaking Areas in Europe Program at the Foreign Service Institute in Washington, DC, from 1999-2000 and President of the International Association for the Study of German Politics from 2005-2010. Dr. Janes has lectured throughout Europe and the United States and has published extensively on issues dealing with Germany, German-American relations, and transatlantic affairs. In addition to regular commentary given to European and American news radio, he has appeared on CBS, CNN, C-SPAN, PBS, CBC, and is a frequent commentator on German television. In 2005, Dr. Janes was awarded the Officer's Cross of the Order of Merit of the Federal Republic of Germany, Germany's highest civilian award.

Kent Logsdon was the Chargé d'Affaires at the U.S. Embassy in Berlin until July 2018 and served as the Deputy Chief of Mission there beginning in August 2015. Prior to coming to Berlin, Mr. Logsdon was the Chief of Staff to the Deputy Secretary of State for Management and Resources in Washington, DC. Prior to this, he served as Deputy Executive Secretary of the State Department. A career member of the Senior Foreign Service, Mr. Logsdon's previous positions include Director of the Operations Center, Director of the Office of Russian Affairs, and Deputy Chief of Mission in Tbilisi, Georgia. He has also served as Political Counselor in Kyiv, Ukraine; and held a variety of positions in Bangkok, Thailand; Almaty, Kazakhstan; and Islamabad, Pakistan. His first tour in the State Department career was at the former U.S. Consulate General in Stuttgart, Germany. Before beginning his professional career, Mr. Logsdon had the opportunity to work as a summer intern in Leverkusen and was an exchange student in Buxtehude. He speaks Russian, Ukrainian, Thai, and German and holds a Master's Degree in International Relations from the University of Virginia and a Bachelor's Degree in Government from the University of Notre Dame.

Gregor Kutzschbach is Head of the Division M5, IT and statistics in the field of migration and asylum, at the Federal Ministry of the Interior, Building, and Community. Dr. Kutzschbach has worked at the Ministry since 2002, working in the fields of data protection; cybersecurity; IT systems of the Federal Police; cyber capacities of the Bundesamt für Verfassungsschutz, the domestic intelligence service of the Federal Republic of Germany; and IT and statistics in the field of migration and asylum. He was previously an attorney at Andersen Legal in Berlin and a Research Assistant in the Faculty of Law at the Humboldt-Universität zu Berlin. He earned a Doctorate in Law from the Humboldt-Universität zu Berlin.

Sarah Lohmann is AICGS' Senior Cyber Fellow and editor of this volume. She coordinates the Institute's cyber projects, including this Transatlantic Cybersecurity Partnership. Dr. Lohmann has also served as a university instructor at the Universität der Bundeswehr since 2010. She achieved her Doctorate in Political Science there in 2013, when she became a senior researcher on the faculty of State and Social Sciences. Prior to her tenure at the Universität der Bundeswehr, she was a press spokeswoman for the U.S. Department of State for the Bureau of Democracy, Human Rights, and Labor, as well as for the Bureau of Near Eastern Affairs (MEPI). Before her government service, she was a journalist, and has traveled in over thirty countries worldwide. She has been published in peer-reviewed journals and books, written and edited several books for internal government circulation, and published over a thousand articles in international press outlets. She is a public speaker in international forums on issues of cybersecurity, defense, and transatlantic relations.

Reinhard Meier-Walser has led the Academy for Politics and Current Affairs at the Hanns-Seidel-Stiftung (HSS) in Munich since 1995. Prof. Dr. Meier-Walser serves as the editor-in-chief of the journal Politische Studien and teaches International Politics at the University of Regensburg. In addition to the theory of international politics, his research and teaching focuses on issues of international, transatlantic, and European security policy. Prof. Dr. Meier-Walser is the author of over 200 publications, including monographs, edited works, and essays in anthologies and professional journals; as well as contributions to newspapers such as the *Neue Zürcher Zeitung*, *Frankfurter Allgemeine Zeitung*, *Süddeutsche Zeitung*, *International Herald Tribune*, and the Austrian newspaper *Die Presse*.

Photo by Jan Kopetzky

Andreas Nick has been a CDU member of the German Bundestag since 2013. He serves on the Committee on Foreign Affairs and is rapporteur for the Council of Europe, the United Nations, issues of global order and cybersecurity, as well as regional rapporteur for Turkey, Hungary, and South America. In addition, he is a substitute member of the Finance Committee and the Digital Agenda Committee. Dr. Nick was elected to the Bundestag following a professional career in banking. His final positions were as head of M&A at Sal. Oppenheim Jr. and Cie. and as professor of corporate finance at the Frankfurt School of Finance and Management. Dr. Nick holds a Master's Degree and a Doctorate in business administration from WHU Otto Beisheim School of Management in Vallendar, as well as a Master of International Public Policy (MIPP) from the Paul H. Nitze School of Advanced International Studies (SAIS) of the Johns Hopkins University in Washington, DC.

Andrea Rotter is a researcher at the Academy for Politics and Current Affairs of the Hanns-Seidel-Stiftung (HSS) in Munich, where she focuses on German security and defense policy and transatlantic security cooperation. She is currently working on a PhD project on differences in transatlantic counterterrorism strategies. Before joining HSS, Ms. Rotter worked as a research assistant for the research division "The Americas" of the German Institute for International and Security Affairs (Stiftung Wissenschaft und Politik, SWP) in Berlin. Prior to that she was an academic assistant and lecturer in the department of International Politics and Transatlantic Relations at the University of Regensburg. Ms. Rotter holds an MA in European-American Relations from the University of Regensburg and a Bachelor's Degree in International Cultural and Business Studies from the University of Passau and the University of Stirling, United Kingdom.

Maximilian Rückert is the director of the digitalization, politics, and media department at the Hanns-Seidel-Stiftung (HSS). He is also a lecturer in the New History Department at the University of Würzburg, where he has been a researcher since 2015. From 2012 to 2015 he received a doctoral scholarship from the Hanns-Seidel-Stiftung.

Bret Schafer is a social media analyst and communications officer at the German Marshall Fund's Alliance for Securing Democracy. He has a Master's in Public Diplomacy from the University of Southern California, and a BS in Communications with a major in radio/television/film from Northwestern University. As an expert in computational propaganda, he has appeared in the *New York Times*, *Business Week*, the *Wall Street Journal*, and the *Los Angeles Times*, and he has regularly been a guest on NPR and BBC radio. Prior to joining ASD, Bret spent more than ten years in the film industry, including stints as a development assistant at the Cartoon Network, a development producer at Citizen Skull Productions, and a freelance writer at Warner Brothers. He has also worked in Budapest as a radio host, and in Berlin as a semi-professional baseball player in Germany's Bundesliga. He is the former editor-in-chief of *Public Diplomacy Magazine*, and his work has been published in the *Chronicle of Social Change*, *LAist.com*, and the *Cipher Brief*, among others. His regional interests are Russia and Central/Eastern Europe, and he previously interned in the Public Affairs Section at the U.S. Embassy in Moscow, Russia.

Matthias Schulze is a cybersecurity expert at the German Institute for International and Security Affairs (Stiftung Wissenschaft und Politik, SWP), where he is the co-coordinator of the cyber research cluster. He currently focuses on cyber conflict, government hacking, encryption, and vulnerability disclosure. He holds a Master's Degree in political science, sociology, and philosophy and defended his Ph.D. thesis "From Cyber-Utopia to Cyber-War. Normative Change in Cyberspace" in August 2017.

Scott W. Tousley is the Deputy Director of the Cybersecurity Division, a part of the Department of Homeland Security (DHS) Science & Technology organization. He helps lead over 40 personnel and holds around $90 million annual research portfolio focused on many aspects of cybersecurity, supporting DHS Components, other government agencies and organizations, and national critical infrastructure sectors. Key areas of this RDT&E portfolio address Cyber Forensics, Insider Threat and Anonymous Networks and Currencies; Cyber-Physical systems and the "Internet of Things"; Mobile Systems cybersecurity; Software Security and Assurance; Critical Infrastructure Security and Resilience; Identity and Privacy; Cybersecurity Education and Training; and many other areas. Working with NIST/Sokwoo Rhee, Scott is helping to lead the GCTC Smart and Secure Cities and Communities Challenge. He served twenty years as an Army officer in the Corps of Engineers, many of these years in interagency technology programs, including the InitialWatch/Warning Unit Chief of the FBI/National Infrastructure Protection Center, part of the Clinton administration's early engagement with national cybersecurity challenges. His experience also includes managing the operations security team for a large Internet Service Provider, principal with a technology start-up company in the private sector, and program manager for MITRE support to the DHS National Cybersecurity Division. He holds graduate degrees in nuclear engineering from Texas A&M, and national security strategy from the Army Command & Staff College. Mr. Tousley has served ten years with DHS, principally with S&T but also with the Domestic Nuclear Detection Office and several other parts of DHS.

THE TRANSATLANTIC CYBERSECURITY PARTNERSHIP

MATTERS OF URGENT PRIORITY

JACKSON JANES

In January 2018, as the German government was trying to cobble together a coalition, and the U.S. government found itself in a shut down, ten Americans and ten Germans committed to the transatlantic relationship considered how they could make their way to Munich, Germany, to find common ground on cybersecurity policy. The U.S. government opened for business just in time for the U.S. delegation to board their planes and trains, and a pause in the coalition negotiating room allowed Bundestag participation. In the context of three meetings in Munich, Berlin, and Washington, DC, the working group of American and German policymakers from the diplomatic, military, homeland security, legislative, academic, and tech communities met to talk about proposals to address threats posed by cyberwar and digital propaganda.

Current events underscored the urgency of finding a common approach: the foreign espionage and intrusion into the "secure" network of the German Federal Foreign Office; the assessment of the U.S. intelligence and congressional oversight committees that the Russians had indeed targeted eighteen state election systems and gained access to the restricted portions of election infrastructure in several; and that their digital propaganda campaign in the lead up to the 2016 elections was intentional, and Putin-directed. At the same time, drafts of legislation regulating practices in the cyber sphere in both countries had the possibility to drastically impact the citizens, the corporations, the privacy, and the security of the other nation.

Recognizing that both countries are affected by the digital propaganda affecting the democratic process during elections, and that a strong cyber defense is critical for both nations, AICGS' Transatlantic Cybersecurity Partnership with the Hanns-Seidel-Stiftung (HSS) aimed to find agreement in both areas through proposals to: improve information-sharing between the two countries on key cyber threats; increase understanding between the private sector and government entities on best practices for ensuring cybersecurity; and to move the legislative and policy conversation in both countries to ensure standards and infrastructure are in place to protect national and international security. In addition, the national and international legal grey zone for many aspects of cybersecurity made agreement between policymakers of both countries on cybersecurity norms critical.

This volume is a collection of those conversations of the working group members conducted across roughly a half year of meetings on both sides of the Atlantic. While much of the agreement achieved is not able to be published due to the degree of its classification, we invite you to listen in to the conversations we can reflect in these pages, which dance around the edges of a long and deep partnership between both countries. Forewords by Germany's Karsten Geier, a diplomat who has played a crucial role in upholding international law in the cyber sphere for years, and the United States' Kent Logsdon, who has tirelessly advocated for a strong transatlantic relationship, reflect the importance of the bilateral relationship in strengthening cyber norms.

Complementing Mr. Geier's cyber norms contribution, scholar Matthias Schulze came up with a new heuristic that could be used by both countries to rate cyber activities according to whether they are offensive or defensive, and thus when international law could justify a response to an attack or intrusion. Department of Homeland Security's Scott Tousley writes about the important ways to protect critical IT infrastructure, and the importance of cooperation with Germany on securing and operating the Internet of systems.

Further outcomes on information-sharing and cooperation on cyber defense are described by AICGS' Senior Cyber Fellow Dr. Sarah Lohmann, who initiated this partnership and this publication. The legislative debate on both sides of the Atlantic is described in more detail by Hanns-Seidel-Stiftung's Andrea Rotter, as is the way forward on digital propaganda by HSS' Maximilian Rückert.

Dr. Andreas Nick, a CDU member of the Bundestag, and his legislative assistant Inger-Luise Heilmann, describe the legislative debate around digital propaganda in Germany, and what remains to be done. Germany's Interior Ministry's Gregor Kutzschbach addresses the role of the state in responding to digital propaganda, while Bret Schafer of GMF's Alliance for Securing Democracy adds the U.S. perspective on how civil society is a key factor in keeping digital propaganda actors accountable.

We are grateful to HSS' Chairwoman Prof. Ursula Männle, for her engagement in this program and for traveling to Washington to support it; to Prof. Dr. Reinhard Meier-Walser, who directs HSS' Academy for Politics and Current Affairs, for his partnership in this joint endeavor; to MdB Dr. Reinhard Brandl, for his passionate engagement in every workshop and his support of the transatlantic relationship; to Elizabeth Caruth, for her expert handling of workshop logistics; and to Jessica Hart, for editing this volume. Our thanks also go to the U.S. Department of State, the U.S. Embassy in Berlin, and the U.S. Consulates in Munich and Frankfurt for supporting this Transatlantic Cybersecurity Partnership every step of the way.

Jack Janes

Dr. Jackson Janes
President Emeritus, AICGS

WAR IN THE CYBERSPHERE

THE POLYVARIANT THREAT NEEDS INTERNATIONAL COOPERATION!

REINHARD MEIER-WALSER

We live in highly complex times, in which the threats to our countries are more diffuse than ever before. Power blocs have given way to new, asymmetrical power relations of multilateral structures. Terms such as “war,” “enemy,” “alliance,” and “friend” are not as clearly definable in our multipolar world order as they had appeared to be a few years ago. The new information and communication technologies and the increasingly interwoven fields of digitalization and globalization cause us to even doubt the traditional meaning of the terms “attack” and “defense.” What is an attack in a cybersphere without borders? Is a cyberattack a phishing-mail which tries to steal highly sensitive data from protected IT structures, or is this categorized in international law as typical espionage? It wasn’t until the year 2013 that the global community decided that international law applies to the cyber realm.

In 2010, only six to seven countries had the capabilities to launch attacks in the cybersphere. Today it is over thirty. The increase in the number of potential actors in cyberwar has clear reasons: It is cost-efficient, saves resources, and is highly effective in targeting both the IT infrastructure of the military, as well as sensitive civil infrastructures, the stability of political systems, and the economy.

Modern hybrid warfare has diverse facets. In the years 2011 and 2013, there were several cyber intrusions into computer networks of the U.S. Department of Defense in order to steal sensitive information about aviation and surveillance technologies. The computer worm “WannaCry”—developed in a North Korean hacker laboratory—infected 230,000 computers in 150 countries in May 2017 with the intention to extort money by blackmail. The following month, the “NotPetya” attack aimed to destabilize Ukraine and incapacitated every fifth computer there. The 2016 cyber hacks on the emails of the Democratic National Committee meant to interfere with the U.S. presidential election, digital propaganda about the fictional sexual abuse of minors, and hacking into German government networks this year and last were all different forms of this hybrid warfare.

Just as polyvariant as the threats are to nations, is the problem of “non-attribution”; that is, the difficulty of credibly identifying the source of the attack with evidence. Only when it is clear who is behind a cyberattack does international law (jus ad bellum) apply. Such proof is usually impossible in the cybersphere. It has been difficult to discern in the attacks that have been proven to this time whether they came from military or civil sources. Most of the millions of daily attacks with malware come from criminal actors. Therefore, the question of domestic purview remains unanswered. When should criminal investigators or in which cases should the military respond to this plethora of threats? The regulation of areas of responsibility is happening on both sides of the Atlantic, and new security agencies are being built in response.

As necessary as it is to create new national cybersecurity strategies as well as resilience strategies, all government actors must be clear on one thing: None of the challenges today can be resolved by one country alone. They require the effort of those where liberty and democracy are prescribed by their constitution. The necessity of multilateral international structures and platforms for international cooperation in regulation of the cybersphere is based on this foundation.

We must recognize at the current time that multilateral structures are often not effective enough, so that large portions of the population ask: Is the multilateral solution really the one that solves problems, or should there be a return to national solutions?

The Academy for Politics and Current Affairs of the Hanns-Seidel-Stiftung (HSS), together with the American Institute for Contemporary German Studies (AICGS) at Johns Hopkins University, strove to explore the possibilities for transatlantic cooperation between policymakers, government representatives, the private sector, and academia.

This opportunity for an exchange could not have been more timely and should serve as an important contribution to the improvement of information-sharing between Germany and the U.S., and lead toward a deeper mutual understanding between German and American policymakers, and governmental and nongovernmental actors in the area of cybersecurity. The goal of this transatlantic platform for exchange, called the “Transatlantic Cybersecurity Partnership,” was to work together toward analysis-based solutions for the current threats in the cybersphere which affect both countries. This publication will present the results of those discussions.

The Transatlantic Cybersecurity Partnership made an important contribution through its interdisciplinary policy approach to the transatlantic dialogue in difficult times. Thanks for the success of this specialized approach go to Dr. Jackson Janes, Dr. Sarah Lohmann, Elizabeth Caruth, and Jessica Hart at AICGS, as well as the colleagues of the Hanns-Seidel-Stiftung, Andrea Rotter and Maximilian Rückert. The valuable results of this transatlantic cooperation aim to provide the armor for the defense of our common values and free, democratic systems. Dr. Martin Luther King, Jr., said it best when he said: “Those who love peace must learn to organize as effectively as those who love war.”

Prof. Dr. Reinhard Meier-Walser
Director, Academy for Politics and Currents Affairs
Hanns-Seidel-Stiftung

THE FUTURE OF WAR?

KENT LOGSDON

Just as people expect government to defend the physical world, they also expect government to protect the cyber realm. Governments must have the means to hold criminals and non-state and state rogue actors in the cyber world accountable. They must be able to discover, attribute, and disrupt their actions. Governments must also create a resilient and robust digital infrastructure. These dual requirements are at the basis of a new policy in the U.S. known as the “Vulnerability Equity Process.” It evolved out of a series of discussions among U.S. government agencies and the private sector about how we can best protect and defend our cyber interests. The key tenets of this policy are transparency, accountability, and most important, informed dialogue. […] When cyber weapons are developed and implemented without consideration of the damage they can cause or the liability they bring, that impacts us all. The number of recent cyber incidents, in the past year alone, demonstrates the need for enhanced cooperation and a discussion of norms.

What is the correct response to these cyber incidents? Well, there are a number of answers to that question.

First, the United States is not afraid to call out countries and hold governments accountable. We have done that in identifying Russia as responsible for the deliberate NotPetya malware attack against Ukraine.

Second, the United States will use the tools of diplomacy and statesmanship. This includes sanctions as a response to cyber incidents.

Third, we will also use law enforcement. In 2014, the United States indicted Chinese military hackers. Earlier this year, thirteen Russians were criminally charged for interfering in the 2016 U.S. election.

Fourth, at times, our response will include cyber tools. One of the best tools we have to understand and get to the attribution of cyberattacks is our ability to hack back at the hackers.

Finally, we need to fight efforts by authoritarian states that use so-called “cybersecurity” arguments to lock down the Internet and repress their citizens.

And so, let me conclude where I began, with the need for increased cooperation. There are a number of ways we are using diplomacy to try to develop and implement the norms we need for a secure and prosperous cyberworld. And our efforts are stronger if we are united in our approach. That’s why the time invested in this Transatlantic Cybersecurity Dialogue, and in our broader ongoing transatlantic dialogue, is so important.

This text is adapted from Mr. Logsdon’s speech in Munich on March 15, 2018, at the Transatlantic Cybersecurity Partnership’s second conference.

COUNTERING THREATS TOGETHER IN THE CYBERSPHERE

KARSTEN GEIER

When the Internet was created, engineers, users, and even political decision-makers were full of idealism. Yet such benign uses of information and communication technology (ICT) are not the whole story. More and more states are using ICT as a means of international conflict. Consequently, the enormous benefits for economic growth and prosperity cyberspace offers are accompanied by risks of escalation and retaliation. Massive denial-of-service attacks, damage to critical infrastructure, or other malicious cyber activity that impairs the use and operation of critical infrastructure have a destabilizing effect on international peace and security. Cyber-enabled interference in democratic political processes also gives reason for concern.

Transatlantic partners have been seeking to address this development. NATO warned at the 2014 Wales Summit that cyberattacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. Allies affirmed that cyber defense is part of NATO's core task of collective defense.

Such warnings must be flanked by a global understanding of the rules for responsible state behavior in cyberspace. The G7 partners committed themselves to contribute to international cooperative action to this end in the 11 April 2017 Lucca Declaration on responsible State Behavior in Cyberspace.

We also need to move forward our work in the United Nations. Since 2005, the United Nations General Assembly has mandated a series of Groups of Governmental Experts to work on this issue. Over the years, these groups have arrived at important conclusions, affirming that international law, and in particular the UN Charter, is applicable and is essential to maintaining peace and stability, offering not only insights on how existing international law applies, but also voluntary, non-binding norms of responsible state behavior to reduce risks to international peace, security, and stability.

Nevertheless, deeply held, worrisome divisions between nations on the use of ICT persist. Their resolution will be fundamental to creating an ICT environment that is open, secure, stable, accessible, and peaceful. There is a need to retain progress made, to continue the discussion in the United Nations, and to increase transparency and inclusivity. Global issues such as this require a global understanding of the threat situation and ways of addressing and mitigating these threats. In this atmosphere, it is more important than ever that allies, including the United States and Germany, work together to find common solutions to countering such threats in the cybersphere.

CONFIDENCE BUILDING IN AN ERA OF DISTRUST

BABY STEPS TOWARD A STRONGER CYBER DEFENSE

SARAH LOHMANN

In the era of distrust that has followed the Snowden revelations, changing administrations, and a transatlantic relationship that is publicly unraveling, “confidence building measures” (CBMs) is a loaded term. In early 2017, when the idea for this partnership was born, the bilateral cyber dialogue between the U.S. State Department and the German Federal Foreign Office had been put on ice. By June 2017, negotiations in the leading forum for discussing cyber norms, the United Nations Governmental Group of Experts (UN GGE), had stalled due to disagreements on interpretation and implementation of the agreed cyber norms as portrayed in its 2015 report.[1]

Yet targeted intrusions into the networks of both countries, sometimes by the same foreign actors, made cooperation between the two countries even more urgent. Agreement on CBMs—the benchmarks for the baby steps that each country takes to show that it is implementing concepts it has agreed on—could not be left for a fair-weather day while espionage attributed to foreign government actors had compromised the networks of Germany’s Federal Foreign Office, and the state election system infrastructure in the United States.

While the Organization for Security and Cooperation in Europe (OSCE) had pounded out quite a detailed list of CBMs in years past, these had not been formally adopted by governments.[2] A forum was urgently needed that could provide a space for further negotiation to ensure that allies could work together to help each other with attribution, accountability of bad actors, and early warning.

This Transatlantic Cybersecurity Partnership, which brought together cyber experts from the U.S. State Department, Germany’s Federal Foreign Office, USEUCOM Joint Cyberspace Center, the German Ministry of Defense, the U.S. Department of Homeland Security, the German Interior Ministry, the Bundestag, Congress, academia, and the private sector, provided a first step. The aim of the group was not to address all stalled CBMs of the past GGE agreements, but rather to find consensus in the areas most urgent to the current cyber defense challenges and to the German-American relationship.

In AICGS’ cyber defense working group, several CBMs were the focus of the discussion:

1. establishing the best fora for information sharing on cyber threats and attribution (falling under the category of “communication and information exchange” in the GGE context);

2. coordination and communication about the legislative process; and

3. establishing common definitions for when the use of a cyberattack is legitimate in coordination with international law (jus ad bellum) and how that force can be used (jus in bello).[3]

Additional confidence building measures discussed during the workshop were ways to protect critical infrastructure from Information and Communication Technology (ICT) threats and to build resilience, and steps toward having a common understanding of the application of international law to the use of ICT to not exacerbate international conflict.

This contribution addresses the working group's outcomes on information-sharing, while Ms. Rotter's text focuses on the dialogue around the legislative process and Mr. Schulze's essay on the common definitions the group discussed. Mr. Tousley shares ideas for protecting critical infrastructure.

Information Sharing Is Best If It Stays Operational

While allies have many levels of analysis where close communication is valuable, this group focused on improving information-sharing modalities on attribution for a malicious cyber intrusion, potential cyber threats, and indicators of compromise. The working group agreed that information-sharing on those topics can happen between Germany and the United States best if it stays on the operational and technical level. Information-sharing between and across countries is easiest when it happens, for example, between military branches, and stays separate from intelligence, participants argued, as this keeps political considerations separate from the technical analysis. At the same time, participants agreed that the aim should be closer cooperation on information-sharing across agencies to defeat stove-pipe mentalities that look only at one analysis.

To strengthen confidence building measures in the cybersphere with allies on the diplomatic front, participants agreed that joint exercises on operational cybersecurity should be undertaken between Germany's Foreign Office and the U.S. Department of State in the near future. Such joint exercises already occur regularly on the military front in the context of NATO, among other venues.

Closer cooperation across the corporate sector and government on cyber threats and solutions is highly desirable, the participants agreed. However, information-sharing connected to the Vulnerability Equities Process, the process that guides when the government tells a software vendor about zero-day vulnerabilities they have discovered in their products, will remain a topic for future discussion.[4]

New Centers of Coordination Needed

Rather than agencies working alone and duplicating work in both countries, the working group proposed a "Cyber Defense Center Plus" as a forum to serve as a conduit for information on cybersecurity internationally. The Cyber Defense Center in Germany is already mandated to act as a hub to bundle data on cyber threats from police, military, and the intelligence community. The proposal would add an international communication arm to coordinate information-sharing with allies.

Such coordination is urgently needed on both sides of the Atlantic. In the United States, there is currently no White House cybersecurity coordinator or homeland security advisor with a cybersecurity focus, but there remains an abundance of government agencies tasked with protecting the nation's cybersecurity or coordinating policy on it at home or abroad. These include: the National Security Council, the Department of Homeland Security, the Department of Justice acting with the Federal Bureau of Investigation, the Office of the Director of National Intelligence, the U.S. Cyber Command Center, and the U.S. Department of State, to name a few. A new Integrated Cyber Center and Joint Operations Center aims to deal with some of those challenges. The new center, opened May 4 by the U.S. Cyber Command and the National Security Agency, provides command and control, and integrates cyber operations across U.S. agencies and with foreign partners. The new center became operational in August and allows different government agencies and foreign allies to sit together under one roof and synchronize cyber operations.[5] While this new center may not address the working group's concern that information-sharing happens on the operational level and stays separate from intelligence agencies, it does provide the opportunity for improved transatlantic information-sharing and stronger mutual operational cyber defense.

Going forward, participants suggested that Germany and the United States undertake a division of labor on identifying threats and analysis of attribution using Open Source information and Early Warning tools available in both countries. This would allow more timely response to malicious cyber incidents, as well as more effective prevention of damage caused by cyberattacks.

Proposing divisions of labor, inviting foreign partners to coordinate operations, sharing hub space and pertinent information on malicious actors, and calling those actors to account: These are the hallmarks of seventy years of the German-American partnership, reflected in a new and creative way in the strong proposals of the working group participants. In the realm of cybersecurity, that partnership is just beginning. In an era of distrust, a transatlantic cybersecurity dialogue will remain vital to keep cyber defense in both countries strong, and to help the bilateral relationship flourish.

NOTES

[1] Elaine Korzak, "UN GGE on Cybersecurity: The End of an Era?" *The Diplomat*, 31 July 2017. Online.

[2] Patryk Pawlak, "Confidence-Building Measures in Cyberspace: Current Debates and Trends" in *International Cyber Norms: Legal, Policy & Industry Perspectives*, ed. Anna-Maria Osula and Henry Rõigas (Tallinn: NATO CCD COE Publications, 2016), pp 136.

[3] For a reflection of the GGE discussions around jus ad bellum and jus in bello, see: Ibid, p. 131, and for information sharing and legislation coordination, see: Ibid, pp. 134-142.

[4] Teodora Delcheva and Stefan Soesanto, "Time to Talk: Europe and the Vulnerability Equities Process," European Council on Foreign Relations *Commentary*, 21 March 2018. Online.

[5] Mark Pomerleau, "Cyber Command, NSA open new $500 million operations center," *Fifth Domain Cyber*, Sightline Media Group, 7 May 2018. Online.

REGULATION IN THE CYBERSPHERE

INTERNATIONAL AND NATIONAL DEBATES

ANDREA ROTTER

A new hack on the German Bundestag at the beginning of 2018 caused a sensation and again brought the explosive nature of cybersecurity policy challenges to the forefront of the debate in the media and in politics.[1] While that intrusion was a form of espionage, cyberattacks can certainly be used as a means of hybrid warfare. Though these occur below the threshold of a military conflict, it is still important that they receive an adequate response. Not only can servers be hacked to gain access to information, but such attacks can also interfere with critical power or telecommunications infrastructures. Moreover, hackers can also target military servers, as attacks in both Germany and the U.S. have already demonstrated. This endangers the operational capability of armed forces in case of emergency and thus represents a serious threat to national security. In addition, these opportunities are no longer limited to state actors, but can also be implemented by non-state actors, thus adding complexity to potential threat scenarios.

Looking at the current proliferation of offensive cyber capabilities, it becomes clear that cyber operations will significantly affect the nature of future conflicts. According to the UN, it is estimated that around thirty states are currently developing or already have offensive cyber capabilities.[2] In addition, cyberspace operations offer the potential attacker advantages that he does not have in the conventional sphere: Cyberattacks are not costly. In contrast to conventional weapon systems, no complex hardware is required, only the necessary software with the corresponding know-how. Moreover, cyberattacks are not constrained by territorial borders. Hackers have the ability to attack a country's critical infrastructures several hundred miles away and conceal their actual location in various ways, making attribution and a timely response almost impossible. The validity of historically-proven deterrence strategies is therefore called into question.

NATO, for example, sought to address this evolution by declaring cyberspace an official area of operation alongside sea, air, and land, elevating cybersecurity to a core task of its collective defense at the 2016 NATO Summit in Warsaw. Thus, a cyberattack could theoretically also trigger a case of mutual self-defense under Article 5 of the NATO Treaty.[3] Due to the potential for uncontrolled escalation of conflicts in cyberspace, states, non-state actors, and science and business representatives are trying to regulate cyberspace. The 2016 "White Paper on German Security Policy and the Future of the Bundeswehr," for example, sets the goal of reaching "a common understanding on the application of international law to the cyber and information domain."[4] However, as with past technological developments, national legislation and the application of international law in cyberspace are lagging behind.

The International Debate

On an international level there are different fora which seek to create a unified approach to cyberattacks. One product of these fora was the Tallinn Manual. In 2009, an international panel of experts coordinating with the NATO Cooperative Cyber Defense Center of Excellence (NATO CCD COE) in Estonia sought to develop international guidelines for cyber-based warfare for the first time.

While the focus in the first "Tallinn Manual on the International Law Applicable to Cyber Warfare" in

2009 was on cyber activities in armed conflict, the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" published in 2013 concentrated on how international law should be applied to cyber operations in peacetime. Though the Tallinn Manuals provide the most complete examination of the international law framework for operations in cyberspace, they only present recommendations by experts, not a consensus built between states and of binding character under international law.[5]

The GGE sessions in the context of the United Nations (UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security) provide the most comprehensive cyberspace regulation mechanisms with state participation to date. Under the UN mandate, there have been five working groups set up in the years 2004/2005, 2009/2010, 2012/2013, 2014/2015, and 2016/2017 in order to cooperate on establishing international yet non-binding norms in cyberspace. The final report of the 2012/2013 process was celebrated as a breakthrough, as a consensus emerged that "international law and in particular the United Nations Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment" among the fifteen participants, including the U.S., Russia, China, Great Britain, France, and Germany.[6] Consequently, the permanent members of the UN Security Council as well as ten other countries agreed that international law is indeed applicable to the cybersphere.

In 2017, however, this process came to an abrupt end. Under Germany's chairmanship, a new GGE of twenty-five experts came together to confer about possible challenges and risks in the area of IT security, as well as strategies to overcome these threats, yet without inhibiting the free flow of information.[7] Unfortunately, in the context of the 2016/2017 working group, there was no consensus reached about a common final report, which caused the UN-led process to flounder. The failure was based on basic differences on the application of international law in the cyber realm. While the U.S. hoped for a definitive position on the application of international law as it relates to self-defense, international humanitarian law, and allowable responses to cyberattacks, countries like China, Russia, and Cuba refused such guidelines. Instead of creating rules applying to conflict, these countries would rather have focused on preventative measures to avoid such conflicts in the first place.[8] There are further multilateral fora outside of the UN framework that work on international cyber norms (for example, within the Shanghai Cooperation Organization under the leadership of Russia and China) or that focus on confidence building measures (i.e., within the OSCE). However, there is still no international consensus about cyber norms, let alone binding international law.

With this background on the faltering progress at the international level, bilateral dialogues and the compatibility of national law initiatives are becoming more important. This gave the Hanns-Seidel-Stiftung (HSS) and the American Institute for Contemporary German Studies (AICGS) at Johns Hopkins University further reason to initiate a Transatlantic Cybersecurity Partnership, in which the relevant German and American actors from academia, politics, the private sector, and the cabinet ministries could be given space to deepen a German-American dialogue and provide concrete policy proposals.

National Discourses in Germany and the U.S.

The different perspectives of threats from the cybersphere, which prevent a global consensus on how to respond to them, can be seen even between allies such as Germany and the U.S. in their differing national strategies. These differing views also expressed themselves during the course of the Transatlantic Cybersecurity Partnership. The possible responses to a cyberattack in peacetime were at the center of the discussion about cyber norms.

Generally, there was consensus that there should be more legislative debate on both sides of the Atlantic about cyber threats. In terms of international norms, Germany is anchored in an EU framework, similar to the United States' Cyber Diplomacy

Act of 2018, which focuses on the development of international cyber norms and encourages U.S. international cooperation in this sensitive area.[9] On the national front, the participants were unified that the countries need to focus on minimizing their own vulnerability and strengthening public-private partnerships (PPP). In the event of a successful cyber-attack, a diversity of methodological responses can be explained by differences in each political culture, the composition of the security apparatus, the legislative framework, and the resulting competencies and the extent to which they are embedded in international frameworks. Germany and the United States set different priorities in the discussion around hack backs and the role of the state and the private sector. On the one hand, Germany wants to leave the regulation authority to the federal state (see the IT-Security Law 2015 and the Cybersecurity Strategy for Germany 2016), but the possibility of active cyber defense by the federal state is currently being evaluated. In the U.S., on the other hand, in the drafted Active Cyber Defense Security Act, legislators are thinking about allowing corporations and organizations that have been attacked to take active cyber defense measures themselves in order to get back stolen information.[10] Of course, according to the draft law, state agencies such as the FBI's National Cyber Investigative Joint Task Force must be informed, but the possibility of independent active measures taken by private actors would be far beyond what is being discussed in Germany. These different legislative initiatives discussed during the workshops provided reason to debate the definition and classification of cyber-attacks, the problem of attribution, as well as what would constitute a measured response to a cyber-attack.

In summary, both countries are relatively at the beginning of the legislative debate around cyber defense. Legal and structural requirements are being applied to developments in the cybersphere step by step. When one considers the common security risks, a German-American dialogue is of absolute necessity. Though many of the questions posed in the framework of the Transatlantic Cybersecurity Partnership could not be answered with certainty, the identification of shared relevant questions, provided added value and inspiration for future rounds of consultation.

NOTES

[1] Georg Mascolo and Ronen Steinke, “Regierung ließ russische Hacker monatelang gewähren,“ *Süddeutsche Zeitung*, 1 March 2018. Online.

[2] See also: “UN GGE” on Geneva Internet Platform Digital Watch Observatory, June 2017. Online.

[3] “Wales Summit Declaration,” NATO, 5 September 2014. Online.

[4] “Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr,” Bundesministerium der Verteidigung, 2016, p. 82. Online.

[5] See also Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

[6] “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A 68/98*,” United Nations General Assembly, 24 June 2013. Online.

[7] “Resolution adopted by the General Assembly on 23 December 2015 A/Res/70/237,” United Nations General Assembly, 23 December 2015. Online.

[8] See: Alex Grigsby, “The End of Cybernorms,” *Survival* Vol. 59 No. 6 (December 2017-January 2018): 109-122.

[9] Cyber Diplomacy Act of 2018 (H.R. 3776), 115th Congress Second Session, 28 June 2018. Online. Passed by the House of Representatives, but not by the Senate.

[10] See: “IT-Sicherheitsgesetz,” Bundesamt für Sicherheit in der Informationstechnik, 15 July 2015. Online; “Cybersicherheitsstrategie für Deutschland 2016,” Bundesministerium des Innern, 9 November 2016. Online; Active Cyber Defense Certainty Act (H.R. 4036), 115th Congress First Session, 12 October 2017). Online.

CRITICAL INFRASTRUCTURE SECURITY, RESILIENCE, AND THE INTERNET OF SYSTEMS

A U.S. PERSPECTIVE

SCOTT W. TOUSLEY

Pervasive and still-growing global connectivity continues to shape and change our world, our economies, our societies, and many elements of human behavior. Along with devices and their software and applications, the underlying infrastructure and critical infrastructure enabling this connectivity continues to grow in both size and complexity, driven by societal and economic demand and innovation. Most elements of this growing "Internet of systems" remains vulnerable to attack, which means all nations and organizations must consider the growing risks present in an ongoing environment of growth and vulnerability. The United States faces perhaps the largest challenge from these risks because of its size and advanced technological and social complexity. Its challenges are reflected elsewhere, in countries such as the United Kingdom, Sweden, the Netherlands, Israel, South Korea, Japan, Australia—and Germany. In this area of challenge—securing the growing Internet of systems—both the United States and Germany should understand and learn from each other because valuable lessons can be drawn in both directions.

This author sees the foundational challenge as the weak and inconsistent quality of many areas of the Internet of systems—design, implementation, operations, awareness, training, etc. Most areas are not good enough or fit enough for their growing economic and social purposes. We also do not have a realistic option of replacing major areas and elements, so we face the most difficult challenge of raising the quality of what we have and operate now, and of steadily building a strong culture of the growing Internet of systems quality. Different countries may find different ways of improving their Internet of systems quality, so we should all look for successes wherever they may be, and it may be that the long-standing reputation for German industrial efficiency and quality can show us ways of how to improve.

In 2013, the U.S. government published major new guidance (Executive Order 13636/Presidential Policy Directive 21) addressing Critical Infrastructure Security and Resilience (CISR). This generated a 2015 National CISR Research and Development Plan, and the five priority areas identified in this plan provide good insight to how we might build up the quality of our Internet of systems and Critical Infrastructure. These include: foundational understanding of critical infrastructure systems and systems dynamics; integrated and scalable risk assessment and management approaches; integrated/proactive capabilities, technologies, and methods for secure and resilient infrastructure; leveraging data sciences for stronger situational awareness and actions consequences; and building a cross-cutting culture of CISR R&D collaboration.

This final priority area of cross-cutting culture is very important, for two reasons. First, the Internet of systems is impacting every area of our economics and societies, including communications, power, health care, transportation, and government, so every area is seeing a cross-cutting culture of change. And second, education is also a foundational element of the long-term evolution of the Internet of systems challenge. Successful education and training and cultural change are necessarily intertwined.

Another major element of the EO13636/PPD-21 guidance was for NIST to lead development of a

Cybersecurity Risk Framework that can help all the different critical infrastructure areas engage their growing risk management challenges. This framework was completed and has been recently updated and has provided a common foundational approach for different critical infrastructure “sectors”, including electricity, transportation, health care, and communications to raise the quality of their risk management. The framework approach has helped many different critical infrastructure sectors and organizations strengthen their risk management of critical infrastructure security and resilience. However, this approach is not the end of what is needed, because the risk management challenge grows ever more complex, from (A) the growing degree of mobility of the various systems and components, (B) the still-growing complexity and resilience uncertainty of the Internet of systems, and (C) the challenge of managing connected efforts of complex systems design, operations, safety, and security. Some of the recurring difficulties in strengthening our critical infrastructure risk management capabilities include different architectural approaches, strategies, and implementations, so risk management across different critical infrastructure areas and systems remains less standardized than hand-crafted. Second, software quality remains inconsistent and often weak, and every critical infrastructure system is foundationally dependent on the software that operates and secures it. Third, there are difficulties of resiliency, both focusing on known, chronic difficulties versus real vulnerabilities and risks that manifest only occasionally.

For several years, the National Institute of Standards and Technology (NIST) has been coordinating the Global Cities Team Challenge (GCTC), supporting a cross-flow of ideas and experiences for how cities and communities throughout the country (and internationally) have been addressing the Internet of systems challenge across their cities and communities. There are clear connections between critical infrastructure security and resilience, and the security and quality of how cities and communities are growing and leveraging these capabilities. But it is interesting to note that the initial years of the GCTC effort generated little focus or insight about how “smart cities and communities” could be secured, made resilient, and support privacy considerations. This is why the current year GCTC program, guided by NIST and DHS Science & Technology, is focused on the Security and Privacy of Smart Cities and Communities nationwide, again showing the pervasive challenges of the Internet of networks.

Another key challenge is that of the public-private partnership. Most areas of the critical infrastructure security and resilience problem operate astride public and private sector organizations, rather than one or the other. Threats, protection, monitoring, response, and recovery are almost all combinations of public and private sector efforts, against both chronic and infrequent areas of the challenge. However, the foundational motivations of public and private organizations remain different (stability versus profit, as one version), and combination public and private organizations are still early in their development and a small part of our current capabilities. So the public/private organizational construct may remain somewhat limited for some time as a source of capabilities against our Internet of systems challenges.

In many problem areas, we see very real challenges that go by names such as counterintuitive, wild cards, paradoxes, etc. Our Internet of systems and CISR challenges are this way also. Strategies of structure and compliance collide with instincts to innovate and “hack the solution,” and this tension plays out in all areas of security. We must do a far better job measuring our systems and their performance, and yet many areas of our Internet of systems challenges remain not very measurable and reflective of the diffusive principles of entropy. Should we choose to orient more on chronic or infrequent problems, or on the most likely or the most dangerous? Increasingly, what might the insurance perspective about our Internet of things and Critical Infrastructure challenges tell us?

In closing, threats to Critical Infrastructure and the Internet of systems come from many different sources—nation-state organizations, criminal enterprise organizations, and other, more limited threats that can still at times cause great damage. These threats come at the many vulnerabilities of the Internet of systems throughout our countries, economies and societies. And we are usually defending against these threats with a shifting and imperfect combination of public and private sector organizations, against both chronic and infrequent areas of the challenge. Years ago, this author worked with and learned a great deal about the very large capabilities of the civil side of the (West) German military organization, the *Wehrbereichskommando* (WBK), the *Verteidigungskreiskommando* (VKK), and the like. The West German military had developed substantial and flexible military capabilities from both their uniformed and civil areas, a character of defense then that is also critical to leverage today. This is a reminder that there may be some very valuable lessons in talking with our German allies and partners about how they are engaging the challenges of Critical Infrastructure Security and Resilience and securing and operating the Internet of systems.

WHERE DOES CYBER DEFENSE STOP AND OFFENSE BEGIN?

MATTHIAS SCHULZE

It is a well-known platitude that the Internet transcends national boundaries, just as it does domestic and foreign policy. However, when countless information technology (IT) networks are bound together in a global system, and more and more countries understand cyberspace as a domain for warfare, then one must ask the fundamental question of what constitutes offensive and defensive action. Traditional definitions of cyberattacks, such as "actions taken to disrupt, deny, degrade or destroy information resident in a computer and/or network" are too simplistic.[1] This is because, among other things, activities in cyberspace have problems with authentication and attribution of actors and are constantly changing and ambiguous.

A cyberattack is usually latent, as compared with kinetic attacks, such as a rocket that has range and explosion impact characteristics. Code is constantly changeable and has no manifest characteristics. Cyber activities can also be anything from digital vandalism, to cybercrime, political and economic espionage, or disruptive or destructive military cyberattacks. The distinct areas cannot be sharply differentiated from each other. A cyber operation developed originally for espionage can become destructive through adding malware modules, or gains the character of cybercrime through selling stolen data obtained through the cyber operation. The spectacular events of 2017—WannaCry and Not Petya—make clear that the mix of political and criminal goals makes it increasingly difficult to classify the attacks. The constant changeability of cyber operations calls into question many governments' classic division of labor in criminal prosecution, divided between the police and espionage units, intelligence services and defense services, and IT security offices and defense/attack forces.

In addition, in political discourse, specific terms exist, such as "lawful hacking," "active defense," and "hack back," which pose new questions about cyber defense and offense and the territoriality of government activity. For example, if police agencies respond to a cyberattack with a hack back targeting a server in a foreign country using penetrating malware in order to gather evidence, they might inadvertently attack a Command and Control Server (C2) of a foreign intelligence service. This defensive cyber-attack can quickly lead to a political escalation. On the other hand, it would be fatal if a criminal uses government-developed malware to launch a cyber intrusion and the attack is then inadvertently classified as a government attack. For this purpose, the factors that define offensive and defensive actions in cyberspace must be defined. If one reviews the cyber strategies of different countries, one discovers that there is little said on what actually constitutes the difference between cyber offense and defense.[2]

This essay presents an analytical process which helps to classify ambivalent activities in cyberspace. It will be argued that the offensive and defensive classification is dependent on the following factors: Where did the action take place (location)? Why did the action happen (intention)? How and with what means was the operation conducted (modus operandi)? What effect did the action have (effect)? What is the context of the activity? These factors should always be considered together.

Location of the Cyber Operation

Both the EU's Budapest Convention (2004) as well as the U.S.' Computer Fraud and Abuse Act of 1986 state that the non-authorized intrusion into a foreign system should be qualified as illegal. This is a purely perimeter-based definition, which refers to the place of a digital operation, and whether one is legally online in their own network, or that of someone else. According to this definition, defensive activities can be understood as those that secure your own perimeters and take place on your own system. Defensive measures can include technical, preventive measures such as firewalls and anti-virus systems, but also organizational processes such as digital rights management and update policies.[3] The active collection of information through intrusion detection systems, honey pots, "threat intelligence," or the use of Hunter-Teams is usually based in your own perimeter and in your own organization. If an external service provider such as CloudFlare is used to mitigate denial of service attacks, to reroute destructive data ("sink holing"), or to block certain servers or IP addresses, it is no longer merely passive defense, but it still takes place in your own legal sphere and national jurisdiction.

According to this location-based typology, offensive actions are those that take place in a foreign network. This includes spying on foreign IT systems or intruding into their systems, either with malware or social engineering.

Intention of the Cyber Operation

Purely location-based definitions usually ignore the motivation or intention of the cyber actor, which is central for classifying the cyber event. An ethical hacker, who uses an offensive cyberattack to perform penetration testing of a company's network, or to test foreign IT systems' weaknesses, would be classified as a criminal actor according to the location-based definition. Making white hat hackers criminals through vague legal bureaucracy is a huge problem for cybersecurity.

Location-based definitions are blind to defensive actions that happen outside one's own perimeters, as well as to offensive actions taken for defensive purposes. Another grey area is the use of a "beacon," which lures the potential attacker to data in your network that appears to be of special interest, but when the data is extracted, it sends the IP address and the location of the attacking computer back to the data's original owner. Technically speaking, a beacon is malware that infects a foreign computer, but the intention behind it makes it defensive rather than offensive. "Bot vaccination," which includes offensively hacking and forcefully patching a remote-controlled computer, also has a defensive goal. Other offensive actions taken for defensive purposes that fall in this grey area include taking over enemy Command and Control (C2) infrastructure or botnet servers in foreign countries with malicious software. Intelligence services call such actions "active defense," and this includes the observation of a cyber attacker on its own system in order to be prepared for attacks. Active defense via beacons or honey pots does not have to be limited to one's own perimeter.[4]

The reason for hacking is therefore a critical part of the analysis for classifying a cyber intrusion. One can differentiate between ego-driven motives, such as personal gain or infamy; political motives, such as "signaling," propaganda, political espionage, coercion, and retribution; and economic motives, including financial gain and espionage. An interesting phenomenon in differentiating between these motives is called "fourth-party collection," when intelligence service A hacks the C2 infrastructures of intelligence service B, and in the process observes how B is spying on target C.[5] Whether intelligence service B's actions are considered offensive once they are discovered depends on whether they share the information they obtained through espionage with intelligence service A.

The effect of an action is therefore just as important as its motivation, as will be outlined below. Ethical motivations, such as the increase of collective security through forced patching, can be rated through the purity of the motives (deontological ethics), as well as through the consequences of the actions (consequential ethics). The purpose does not always justify the means used, and even good motivations can cause damages, for example, when a computer that has been forcefully vaccinated no longer functions.

Of course, multiple motives can overlap, which is why motivation-based definitions of offensive and defensive actions are not enough. The WannaCry incident from 2017 appeared to be a classic ransomware incident, with the aim of financial gain. In reality, it also had a political objective. The intention of an incident is often not easily determined. Due to ambiguities in the digital sphere, problems with attribution, and the frequent absence of claims of responsibility, the motivations are often not clear and should be regarded with caution. For a cyber defender, it is often not clear whether a hacker is infiltrating a system due to espionage or with destructive motives, which is why often the worst is assumed. Often the indicators of compromise—i.e., the digital footprints—reveal the motivation.

Modus Operandi

Similar to a break-in at someone's home, with a cyber intrusion, the type of action and the choice of means—the modus operandi—illuminates much about the professionalism and implicitly also the motives of the attacker. Thus, analyzing the modus operandi helps with the classification of acts as offensive or defensive. When the goal is to remain undiscovered for the longest possible period, the attacker will put great effort into trying to hide, which, depending on the complexity, often speaks for an intelligence service. Military cyber operations in time-sensitive situations are less interested in camouflage than military targets which can be immediately destroyed. Cyber criminals do not have the financial resources to develop Zero Day exploits, and they therefore use well-known security weaknesses. Cyber criminals frequently use a form of monetization with a large amount of automation, i.e., sending massive numbers of spam or phishing mails. The choice and characteristics of the target and the boldness of the attack, its complexity, and its camouflaging are all parts of the modus operandi of the attacker. The choice of target also reveals much about the motivation behind the incident.

The modus operandi influences the political categorization of an incident and is closely associated with the process of attribution.[6] Without exact forensics and analysis of the incident, valid attribution cannot be made. This is especially important for false flag operations, since with false attribution an innocent third party could be harassed. Pretending to be someone else while breaking into highly sensitive networks of a country might produce more severe political reactions in contrast to cases where an attacker gains access to a network due to a badly configured firewall. The same circumstances play a role in the many cyber incidents occurring around the inadvertent data leaks.[7]

The modus operandi can be determined through the tools and scripts used in a cyber operation. Here there is also a certain ambivalence, so that these criteria should not be used alone. Offensive and defensive cyber operations are based on similar skills and often use the same tools, including those previously installed. This is called "living off the land." Such a circumstance makes the classification of cyber weapons quite complex.[8]

Effect

Just because a system or network has been hacked does not automatically mean that negative consequences should be expected. Most cyber incidents produce only slight, hardly recognizable effects. Many cyber operations successfully penetrate a network but fail when delivering the payload. They fail due to defensive mechanisms, which by definition prevent negative ramifications of an attack.[9] It also can happen that an intruder does not find something in the system that he's looking for and leaves empty-handed. The malicious WannaCry software could have had a greater effect had there not been coding mistakes in the integration of a "kill switch." Alternatively, a successful hack of a honey pot or a fake network is actually a tactical failure if the modus operandi is revealed in the process. For the same reason, a tactical success can also be a strategic failure.

One can also differentiate between quality and scope of an effect. One can differentiate levels of quality of an incident as follows: a temporary interruption, a semi-permanent destruction of data or systems (through a “wiper” module), permanent physical destruction (e.g., Stuxnet), or as the exfiltration and manipulation of data. To produce kinetic effects takes an enormous amount of time and resources and therefore seldom occurs.[10]

A Distributed Denial of Service (DDoS) attack is easier because it lasts just a few minutes, or at the most, just a few days. If a company network stops working due to malicious software, it is often a matter of days or weeks until a backup is up and running and business can return to normal. Political or economic espionage operations usually only produce indirect costs, such as the underestimated psychological effects of the lack of trust in your own system or processes, or negative externalities in the form of insurance costs, and the loss of competitive advantage through the theft of intellectual property.[11]

The Tallinn Manual, which attempts to apply international law to cyberspace, provides a helpful typology for rating the effects of cyber operations.[12] Digital incidents which cause human injury or loss of life, or which damage or destroy physical objects, can be classified as use of force according to international law. Retaliatory actions or the right to defense can be activated when the incident can be compared to an armed attack.

As this is a legal grey zone, the severity, the immediacy, the directness, the invasiveness, the degree to which the effects can be measured, the military character, the state participation as well as the assumed legality must be considered. The severity describes the previously named spectrum from disruption to destruction. Immediate consequences count more than hypothetical losses in the future. The direction describes the units in the chain of causation from source to effect. For example, economic sanctions usually have long-term effects and create collateral damage. An armed, physical attack has direct effects. Collateral damage describes the range of the effects. But system failure in hundreds of countries because of the WannaCry incident can also influence the severity. The more innocents are affected, the worse the incident. The intrusiveness describes the degree to which operations penetrate a state’s critical functionality: the more secure and sensitive a state considers a system, the more invasive it will consider the attack.

The military character can usually be identified through targeting, since militaries usually attack other military systems according to international law, and only attack civilian infrastructure based on the *jus in Bello* concept, when these supply military structures. It is usually difficult to identify whether an operation is state-sponsored or operated. The same goes for the criteria of the assumed legality.

A direct, immediate cyber incident with many visible, long-term collateral effects will be more likely considered an offensive act than a qualitatively smaller and shorter incident such as a DDoS attack.

Context

The phrase “context is for kings” is also applicable in cyberspace. The context of a cyber incident has an immense influence on how these will be politically assessed, and which reactions would be reasonable.

That is why it plays a role if a cyber incident is a singular event or takes place at the end of a chain of events or is part of a longer cyber campaign. Path dependencies of historical events are relevant for classifying cyber incidents. Cyber escalations between two actors who have a history with each other tend to intensify.[13] Cyber conflicts with a longer history can also lead to the problem that each actor knows his enemy’s red line and politically instrumentalizes it.

The gravest contextual condition is the question of whether a cyber operation takes place during peacetime or in the context of an armed conflict. This determines in many countries when certain actors or institutions become active. Military hackers play a role especially in the context of armed conflict. There, the usual international law restrictions apply to cyberattacks in the framework of self-defense, and the victim can either respond in kind or with other methods. Spying on a target through military reconnaissance must be evaluated differently during a conflict than in peace time, where defense against espionage or the law enforcement authorities would call the actions to account.

The subjective, psychological perception of incidents should not be underestimated. The actual damages must be differentiated from perceived damages and must influence whether the victim interprets the cyber incident as offensive.

There is surely an additional long list of contextual factors that should be considered. As with all government activities, interpretation and perception play a role in whether a state sees its own action as aggressive or offensive.

Conclusion

It is difficult to generalize about cyber incidents, because each one has very individual characteristics and contexts. It is no coincidence that cyber forensic companies look at most incidents on a case by case basis, and rarely make inductive generalizations. Quick generalizations and categorizations can lead to mistaken conclusions and to wrong political consequences. Thus, it is difficult to say if a cyber incident was offensive or defensive in nature. Often when there are immediate, visible effects such as physical damages, the judgment seems easier to make. These cases are only a very small minority.

Most cases occur in a hybrid spectrum underneath the threshold of an armed attack. Digital incidents show a high degree of ambiguity and changeability, which is why they can't be put in tight legal frameworks. This is the reason why in many countries there is a question of which agency has purview, for example when an operation mixes criminal and political intent. Would this then be under the law enforcement agency's purview or a job for the espionage defense officials? The question of whether a cyber incident is defensive or offensive is usually based on the combination of the legal, technical, and political analysis of the incident. The three levels of analysis must not be congruent with one another. However, the factors of place, intention, modus operandi, effect, and context of the political classification and determination of response reactions—no matter whether those responses are digital or analogue—must be considered as a whole, and given enough time for analysis.

NOTES

[1] Definition of NATO. See NATO Cooperative Cyber Defence Centre of Excellence (CCDOE) Cyber Definitions.

[2] Belgium defines it as follows: "Offensive capacity includes the manipulation or disruption of networks and system with the purpose of limiting or eliminating the adversary's operational capability." See NATO CCDOE Cyber Definitions.

[3] Sven Herpig, "Hackback ist nicht gleich Hackback," *Stiftung Neue Verantwortung*, 24 July 2018. Online.

[4] *Into the Gray Zone. The Private Sector and Active Defense Against Cyber Threats* (Washington, DC: The George Washington University Center for Cyber and Homeland Security, 2016), p. 6. Online.

[5] Juan Andrés Guerrero-Saade and Costin Raiu , "Walking in your enemy's shadow: when fourth-party collection becomes attribution hell," *Virus Bulletin*, 4 October 2017. Online.

[6] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38 (2014): 4–37.

[7] Due to a false server migration the data of a Swedish transport was exposed for a longer period, meaning viewable on the Internet. This was not a hack in the classical sense.

[8] Christopher A. Ford, "The Trouble with Cyber Arms Control," *The New Atlantis* 29 (2010): 52–67.

[9] Herb Lin, "Fundamentals of Cyber Conflict," Lecture at Stanford University, 23 May 2017. Online.

[10] Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41:3 (2017): 995.

[11] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24 (2015): 8330.

[12] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn: NATO CCDOE, 2013), p. 49.

[13] Anthony Craig and Brandon Valeriano, "Conceptualising cyber arms races," 8th International Conference on Cyber Conflict (CyCon), 4 August 2016, p. 141–158. Online.

THE WAR WITH WORDS

DIGITAL PROPAGANDA AS A MULTILATERAL, MULTI-PERSPECTIVE, AND MULTI-STAKEHOLDER CHALLENGE

MAXIMILIAN TH. L. RÜCKERT

Maxwell Aitken, the first Baron of Beaverbrook (1879-1964), was a successful Canadian-British businessman, a newspaper editor, and, even in younger years, an influential grey eminence in British politics. Given his experience in dealing with money as well as with public opinion, he advanced to the position of the Minister of Information of the British government during World War I. Unlike many of his fellow countrymen, Aitken understood the great significance of the so-called war with words. He considered propaganda the "'popular arm of diplomacy' in which 'the munitions of the mind became not less vital for victory than fleets or armies.'"[1] The "munitions of the mind," i.e., the idea of shaping both domestic and foreign public opinion, were used long before and after his time in office.

Nowadays, the contest for public opinion becomes even more important "as we learn more and more about the workings of the human mind in an era where nuclear weapons could readily destroy all human life on the planet, propaganda and psychological operations (as they are now called) have become genuine alternatives to war."[2] In 2005, former U.S. Secretary of Defense Donald Rumsfeld emphasized the importance of public support during the Iraq war in an interview with the German magazine *Der Spiegel*: "The powerhouse of the Iraq war is not in Iraq. We do not lose battles and skirmishes there. Look, the real battlefields are the public in your country and our country."[3]

The combatants on this battlefield are, of course, not only domestic. The freedom of expression in liberal democratic orders is both one of their fundamental pillars and their Achilles' heel, used by their external opponents. During the Cold War, Russia's dezinformazia aimed at this seemingly weak target, especially in the young German Republic. Disinformation campaigns were aimed at exploiting already existing social cleavages and conflicts, as for example the student movement in 1968 or the peace movement in the 1980s.[4] Meanwhile, China devised its own strategy of influencing narratives in foreign states. It started to create an incrementally more convincing new baseline of its own history. Since then, the perception of the once repudiated aggressive regime of "Cultural Revolution" has significantly shifted in many parts of the world.

Today the public sphere is still a battlefield in Germany, as well as in the United States of America, but in new dimensions: The war with words is fought with binary codes and on a global scale. Via social media channels and often automated bots, malign actors are capable of deliberately spreading disinformation, thereby reaching an audience on a hitherto unforeseen scale.[5] Moreover, as concerns nearly all matters in cyberspace, there are barely any international norms regulating the spread of propaganda, let alone binding rules or solidified sanction mechanisms. This extent of digital propaganda today employed by state and non-state actors represents a common threat for both states.

The Hanns-Seidel-Stiftung (HSS) and the American Institute for Contemporary German Studies (AICGS) at Johns Hopkins University invited many renowned German and American experts representing various professional backgrounds and perspectives on cybersecurity to build a transnational working group to find agreement on norms.

The U.S. and German participants of this working group agreed on common principles, like securing the free democratic order on both sides of the Atlantic, as well as stabilizing and shaping a sustainable future within. This democratic order is at risk following the increase in importance of the role of the digital-marketing industry on the one hand, and the increased use of social media for hybrid warfare on the other. Hate speech, "Fake News," and specific disinformation campaigns target the heart of democracy when they interfere in the free, equal, and secret elections of the parliaments of both nations. The working group subsumed all these threats under the term of "digital propaganda" and pointed out that the focus of the current public and political debate should include many more activities, such as data theft and data security. The response to digital propaganda—retaliation and resilience in a war with words—has to have the same importance and significance in the political agenda as it does in the public discourse.

The German and the U.S. security authorities, as well as the participants of the working group, are aware of the fact that there is not one responsible protagonist in the conflicts related to digital propaganda, but there can only be one common reaction. One-sided blaming on individual social media platforms and the systematic fake news or so-called "Dark Ads" submitted with novel digital marketing tools are wrong and do not lead to finding sustainable solutions. Individual state actors, radical political groups, and other non-state actors that try to destabilize democratic systems by using digital propaganda cannot always be accurately attributed. According to the working group, in times of hybrid warfare online, traditional and stereotyped conceptions of an enemy such as Cold War Russia or Cultural Revolution China are no longer convincing. The concepts of the enemy in the war with words has to be reevaluated.

As a matter of diverse history of law as well as diverse legal practice, there have to be different solutions for the same problems for both nations. Because of that, the working group defined distinct fields of action for both countries to provide solutions for the causes and effects of digital propaganda in the future, to include the media, digital economy, politics and the state, civil society, and individual media skills of the general population. There is no question that every single person in both countries needs a pronounced ability to form his or her own opinion in times of daily information overload.

Relating to the field of "Politics and the State," the working group discussed, for example, the introduction of a "Bot Labeling System," controlled by the state, which would warn the user of possible automation intended to influence readers' perceptions. In addition, the experts agreed that media literacy education is extremely necessary for all ages.

Relating to the field of "civil society" there are various possibilities for both countries. One could be the development of institutionalized "Fact-checking Gateways" as well as the development of state-initiated party-neutral institutions of political education, such as the German Federal Agency for Political Education.

The contributions following in this volume summarize the digital propaganda working group's findings and highlight the action frameworks on both sides of the Atlantic for hybrid warfare in the future.

NOTES

[1] Quoted in David Welch, *Propaganda, Power, and Persuasion: From World War I to Wikileaks* (London: IB Tauris & Do Ltd, 2014), p. 86.

[2] Philipp M. Taylor, *Munitions of the mind: A history of propaganda from the ancient world to the present day* (Manchester: Manchester University Press, 2003), p. 8.

[3] "Wir werden die Dinge richten: Interview with Donald Rumsfeld," *Der Spiegel* 44/2005, 31 October 2005.

[4] See Matthias Schulze, "Hack, Leak, Amplify. Die Wirkungsweise von Cyber-Operationen und Desinformationen im Kontext der US Präsidentschaftswahlen 2016," in *Propaganda als (neue) außen-und sicherheitspolitische Herausforderung*, ed. Torsten Oppeland, Schrifte des Hellmuth-Loening-Zentrums für Staatswissenschaften Jena, Band 24 (Berlin, 2018): 39.

[5] See Lisa-Maria N. Neudert, "Computational Propaganda in Germany: A Cautionary Tale," *Computational Propaganda Research Project* Working Paper 2017(7). Online.

THE PARLIAMENTARY VIEW

PROTECTING OUR SOCIETIES FROM PROPAGANDA AND DISINFORMATION

ANDREAS NICK AND INGER-LUISE HEILMANN

Understanding Disinformation and Digital Propaganda

Today's interconnected societies have largely benefited from the Internet. The world-wide web enables unlimited information sharing, communication, and transactions. Some argue that data has replaced oil as the world's most valuable resource going forward.[1] A whole new data-driven economy has emerged. Ad-based social media platforms and smart technologies such as Artificial Intelligence (AI) have a considerable impact on our societies—on business models, on media companies, and on the privacy of our citizens. From a mere technological viewpoint, digitization is not political as such.[2] Yet it enables new societal practices and thus becomes political.

Policymakers on both sides of the Atlantic have become increasingly aware of the challenges in conjunction with the success and spread of social media. On both sides of the Atlantic, digital propaganda and fake news in particular are regarded as harmful. The United States and the European Union share the experience of targeted disinformation campaigns, the majority being conducted from outside our countries. According to a recent Eurobarometer poll, 85 percent of Europeans view fake news as a problem in their countries, and nearly as many consider fake news a threat to democracy.[3] As Christian Democrats in the German Bundestag, we consider the spread of fake news and targeted disinformation campaigns a challenge to the integrity of our liberal, democratic discourse.[4]

The long-term effects of social media on our society also need closer scrutiny. Historian Niall Ferguson has studied the history of social networks and recently compared the world-wide web to the invention of the printing press more than 500 years ago—with a worrying analogy of its social consequences.[5] Ferguson notes that individualization and massification, the dissemination of fake news, hate messages, and incitement, as well as the rise of religiously-motivated conflicts, increased during the first decades after the printing press was invented and before new rules and standards were established. Drawing from these dynamics, enhancing the resilience of our societies and complementing such measures with new forms of social media regulation should be the first priority from a parliamentarian point of view. Moreover, social media platforms need to take on more responsibility and need to cooperate with the public sector and civil society in order to actively combat disinformation, election meddling, and digital propaganda.

Enhancing Resilience of Our Societies

Digital propaganda and disinformation campaigns aim at undermining institutions and the fabric of society.[6] The most critical task in our democracies is thus to increase resilience in order to be less vulnerable and to better confront new challenges. Resilience demonstrates the ability to resist adversary campaigns, to flexibly adjust and to swiftly recover from disruptions. It needs to be rooted in our minds and our democratic institutions. Enhancing resilience to cope with online disinformation comprises measures by the political institutions and governments, the security sector, the education system, civil society, and social media companies.

Resilience ground work entails a stronger focus on digital literacy. Students of all ages should be able to follow comprehensive media and information literacy courses. They need to understand what algorithms are and how the ad-based business models of social media platforms function. Our society also needs to learn how to distinguish high-quality and trustworthy pieces of information from fake news or mere propaganda. Measurements of media and information literacy could even be added to the OECD's PISA rankings.[7]

Resilient societies also require strong democratic institutions. Political institutions, media, and civil society have to increase their efforts to explain and discuss politics in a credible, transparent, and concise way. Politicians and civil servants need to work toward more effective and credible institutions. Public awareness of digital propaganda or disinformation should be raised concertedly with the media. In acute cases of disinformation campaigns, both governments and media should react in a timely and proportionate way without citing rumors, as otherwise these would receive more attention. Additionally, security agencies, governments, and the media should follow a clearly defined schedule on how to answer acute disinformation campaigns.

A broader understanding of resilience also takes into account technical and organizational resilience. As online campaigns frequently draw on leaks and hacks, both the public and the private sector need to enhance the security of their information systems. Germany, for instance, published a comprehensive cybersecurity strategy in 2016 and established an early-warning system for cyber espionage or attacks. Making societies as resilient as possible also entails secure election systems. In Germany, citizens vote on paper and no voting machines are used. The data is aggregated on computers without connection to the Internet. As a result, experts consider a hacking of voting technology unlikely: "Voters' heads are by far the more vulnerable target," Brookings expert Constanze Stelzenmüller concluded in her testimony before the U.S. Senate Select Committee on Intelligence.[8]

Societal resilience can be further increased by supporting the media in delivering high-quality journalism and sustaining its financing to make it less vulnerable. Moreover, tools such as source transparency indicators or verified content labels could be established by the media to recognize their outlet as trustworthy and to empower citizens. Cooperation between the media and fact-checking institutions also contributes to high-quality journalism and to the debunking of fake news. Above all, reporters need continuous training. They should always check the trustworthiness of their sources and be aware of the agenda behind the information.

Addressing Disinformation and Digital Propaganda through Legislative Means

Measures for more resilient societies and democratic institutions need to be accompanied by concise rules for social media companies and users posting online. When developing social media regulation and drafting legislative proposals in this realm, the main objective should be not to re-invent the wheel, but to draw from existing regulation in related domains.

One option policymakers in Germany and elsewhere should consider more seriously is to apply traditional media law more rigorously in the digital world as well. Social "media" platforms have been exempted from traditional media laws thus far. But they must take on more responsibility as a filter for content quality assurance and therefore must prevent the spread of false information, enforced by law if necessary. As a suitable analogy, we should think of Facebook not as a word processing program or telephone line, but as a medium such as television, radio, or newspaper. Facebook has rejected the idea of being a media company so far, claiming it would just host information, not produce it, as the company intends not to be subject to media regulations. However, as the Facebook algorithm selects stories and pieces of information, Facebook could be considered a media company. Therefore, editorial rules must apply: It should at least be comparable to the task of newspaper publishers that are responsible if inappropriate content was published in the letter to the editor section and they had not met their requirements of examination. In Germany, the discussion on the right to rebuttals, a concept borrowed from German press law, has not yet come to a conclusion on the federal level as press law lies in the realm of the German states. However, existing technological possibilities need to be utilized to post rectifications after users have seen posts of fake news or disinformation.[9]

First concrete initiatives have been launched in order to address disinformation and digital propaganda. The European Commission, for instance, convened a Multistakeholder Forum on Disinformation to develop a Code of Practice (CoP) that should serve as a self-regulatory framework for online platforms and advertisers. It should include inter alia more transparency about sponsored content and political ads and detailed information on algorithms that prioritize the display of content as well as labels and rules for bots and the fight against fake accounts. It will further demand social media platforms to improve "the findability of trustworthy content."[10] The EU-wide CoP are supposed to produce tangible effects in the months following its publication. If these results are not satisfactory, the Commission plans to take other steps that might include regulatory measures.

With the Network Enforcement Law, passed in 2017, Germany has taken a first important step against hate speech on the Internet. The reasoning behind this law was that international social media companies have to comply with the German legal order if they make their services accessible to German users. The social media companies are thus responsible for what happens on their platforms. However, this can only be a first step in the field of social media regulation. Social media platforms also should provide more transparency about their business models and algorithms in order to aid researchers in closing research gaps.[11] Furthermore, social media platforms should provide more information about the sponsors of political advertising, the amount spent on the political ad, as well as targeting parameters.[12] Possible future legislation should also consult anti-trust regulation so that big social media platforms cannot abuse their market power to react very slowly to the demands by civil society and political institutions.

Establishing a Long-term Understanding about Disruption in Our Societies

New forms of regulation and measures to increase resilience are the two main areas in which national parliaments can act against disinformation and digital propaganda. Quick fixes, however, would not be desirable; sustainable multi-stakeholder engagement is required instead. The long-term effects of social networks on our society as a whole need further investigation by the academic and the political spheres. New regulation can only be developed on the basis of a deeper understanding about the impact of social media platforms. On that basis, legislation about media law and anti-trust regulation will need to be adopted.

Apart from disinformation and digital propaganda, other fields for social media regulation have been widely discussed following the Cambridge Analytica case. Data protection concerns have been central to the European reaction to the scandal. Data protection is a fundamental right enshrined in the EU Charter of Fundamental Rights (Article 8) and needs proper enforcement.[13] Another issue for consideration could be to subject social media platforms to the secrecy of telecommunication if they provide telecommunications-like services. This could also include the application of data retention laws to social networks, implying that personal data might be saved for no longer than 90 days.

A wide array of areas need legislative clarification—the transatlantic exchange on common challenges and possible solutions therefore remains vital. On the parliamentarian level, we could foster cooperation through more institutionalized formats. Taking concerted measures to enhance resilience in our societies would make it harder for adversaries to undermine confidence in democratic institutions or to generate confusion via online campaigns.

NOTES

[1] "Data is giving rise to a new economy. How is it shaping up?" *The Economist*, 6 May 2017. Online.

[2] Daniel Jacob and Thorsten Thiel, "Einleitung: Digitalisierung als politisches Phänomen," in *Politische Theorie und Digitalisierung*, eds. Daniel Jacob and Thorsten Thiel (Baden-Baden: Nomos, 2017), p. 8.

[3] European Commission, "Final results of the Eurobarometer on fake news and online disinformation," 12 March 2018. Online.

[4] CDU/CSU-Fraktion im Deutschen Bundestag, "Diskussion statt Diffamierung Aktionsplan zur Sicherung eines freiheitlich demokratischen Diskurses in sozialen Medien," CDUCSU.de, 24 January 2017, p. 2. Online.

[5] James Homann, "How Zuckerberg's Facebook is like Gutenberg's printing press," *The Washington Post*, 28 March 2018. Online.

[6] Andrew Weisburd, Clint Watts, and JM Berger, "Trolling For Trump: How Russia Is Trying To Destroy Our Democracy," *War On The Rocks*, 6 November 2016. Online.

[7] European Commission, "A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation," 12 March 2018, p. 27. Online.

[8] Constanze Stelzenmüller, "The impact of Russian interference on Germany's 2017 elections," Congressional Testimony, The Brookings Institution, 28 June 2017. Online.

[9] CDU/CSU-Fraktion im Deutschen Bundestag, "Diskussion statt Diffamierung Aktionsplan zur Sicherung eines freiheitlich demokratischen Diskurses in sozialen Medien," CDUCSU.de, 24 January 2017, p. 6. Online.

[10] European Commission, "Tackling online disinformation: a European Approach," COM 2018 236, European Commission, 26 April 2018, Section 3.1.1. Online.

[11] Alexander Pirang, "Germany's Half-Baked Approach to Fighting Disinformation," GPPI Commentary, 12 April 2018. Online.

[12] Ben Scott and Dipayan Ghosh, "Digitale Werbung und politische Propaganda: Wie mit Technologien der digitalen Werbeindustrie Desinformation im Netz verbreitet wird," Stiftung Neue Verantwortung, March 2018. Online.

[13] European Parliament, European Council and European Commission, "Charter Of Fundamental Rights Of The European Union," 2012/C 326/02, EUR-lex, 26 October 2012. Online.

DIGITAL PROPAGANDA AND CYBER THREATS

THE ROLE OF POLITICS AND THE STATE

GREGOR KUTZSCHBACH

Politics and the state are facing new challenges posed by digital propaganda and cyber threats since the obvious aim of those digital propaganda campaigns and cyberattacks is to undermine democracy, to weaken the credibility of the government and the elected, and to jeopardize state institutions and critical infrastructures. There are several ways for governments to counter digital propaganda, "fake news," and cyber threats posed by state actors, although governmental institutions can sometimes only provide a small contribution to the solution of this problem.

Digital Propaganda

As far as digital propaganda is concerned, the so-called "Lisa Case" in Germany illustrates that official statements won't stop a good fake news campaign (see next page). People who—for whatever reason—believe that the authorities are against them or not willing to protect them will trust in the rumor-spreading campaign rather than officials denying those rumors.

However, that does not mean that official statements aren't crucial for the damage digital propaganda may cause. Bad public relations on the official side may even fortify the propaganda campaign. Therefore, a conclusion one should draw from the "Lisa case" is that official communiques should be quick, transparent, and accurate. If the official reaction to serious rumors comes too late, this will be understood by some people as a confession of guilt. The withdrawal of information, even if for the best of reasons, as well as the fact that authorities may have to correct their statement later on, may be taken as an affirmation of the rumors.

This is nothing new and has been true for "offline propaganda" as well. But thanks to social media and electronic forms of communications, digital propaganda and fake news spread much faster and can reach more people in the target audience than before. This means that authorities have to react much more quickly and precisely when accusations start to spread via social media channels. The government and authorities should make every step and decision transparent and comprehensible to the furthest extent possible.

Although the possibilities to react directly in this battle of information and propaganda are limited for authorities and politicians, there still remain some fields of activity on which the state may act.

People are more vulnerable to digital propaganda the less they are informed about democratic institutions, the political system, and the constitutional state. Since people cannot be forced to read or learn about these things, the state can at least provide influencers like teachers, local politicians, NGO activists, and other "active citizens" with information and educational material.

For instance, in Germany the German Federal Agency for Civic Education (Bundeszentrale für politische Bildung, BPB) was established in 1952 in order to educate the German people about democratic principles and prevent any moves to re-establish a totalitarian regime. It provides citizenship education and information on political issues to all people in Germany. To foster an awareness of what democracy is and to encourage participation in politics and social life, the BPB publishes books, leaflets, films, and other educational material on the major issues of our times and

“LISA CASE”

Lisa was a girl who, according to the outcome of the official investigations, ran away from home for one day and stayed at a friend’s place where they had sexual intercourse. Since she was only 13 at this time, this person later was charged with sexual intercourse with a minor and producing child pornography. Since “Lisa” and her family were immigrants from Russia, Russian media, especially RTV, started a campaign saying that she was kidnapped and raped by refugees, which rapidly spread throughout social media channels. Even the Russian Minister for Foreign Affairs Sergey Lavrov gave a statement and accused German authorities of covering up the crime. This narrative took place in January 2016, the year after nearly a million refugees from Syria and other mainly Arabic countries came to Germany. The local police authorities quickly denied that the girl had been kidnapped or even raped, but nevertheless the campaign went on and led to concern, agitation, and even demonstrations within the local group of Russian immigrants. The rumors were fueled by the fact that the authorities in the first statement denied that any crime had been committed, but later had to clarify that they were investigating a criminal case of sexual intercourse with minors. The police justified the initial statements with their aim to protect the girl.

in all areas of politics. This is not the only way the state can encourage citizens to engage in the democratic process. A lot of political and scientific foundations, institutes, and other NGOs have devoted themselves to political education. In helping to fund these institutions—in a way and with an amount of money that does not challenge their independence—the state can contribute to these goals without having to engage directly in this field.

Another example is the public service broadcasting system in Germany (and other European countries like the BBC in the UK). The idea of a public service broadcasting system is that those broadcasting stations are—unlike private enterprises—funded by taxes or fees and do not have to rely on advertising revenue to finance their program. In return, the public service broadcasting systems are obliged to provide citizens with politically neutral or well-balanced information on political, educational, and cultural issues. To maintain their political independence, there are several safeguards in place to prevent politicians or governments from influencing the program and news coverage, bearing in mind the misuse of state-owned media for state propaganda during the Third Reich in Germany.

A new and completely different approach to foster civil society in the age of social media and digital communications in Germany is the Network Enforcement Act (*Netzwerkdurchsetzungsgesetz*). This legal act was adopted by the German parliament in 2017 and went into force on January 1, 2018, is the reaction of the German legislature to the increasing amount of hate speech, fake news, and illegal content in social networks. The aim is not to prohibit this content, which is already illegal anyway, but to encourage the social media providers to do more to prevent this illegal content from being distributed through their services.

One of the main principles of German telecommunication and internet law is that access and content providers cannot be held responsible for third-party content distributed throughout their networks. They are only obliged to delete questionable content if they are informed about it by someone or if it comes to their attention in some way. Since the legislature observed that too much illegal content stays online for too long, the new law obliges social media providers to maintain a functioning system to alert, identify, and delete illegal content. If they provide their services in Germany or to German customers, they have to react to each notification of illegal content and have to make sure that obviously illegal content is deleted within 24 hours and all other illegal content within 7 days. High fines of up to €50 million are possible in cases of non-compliance.

The Network Enforcement Act was controversial in the public discourse. The criticism focused on the fact that the providers may be forced to act as a judge instead of the courts and that they may tend to "overblock" content in fear of the high fines for not complying with the law. But after the first seven months it can be stated that these worries were baseless: The amount of content deleted due to the new law is very low compared to the content deleted for other reasons, especially for non-compliance with the terms of use. And there have been virtually zero complaints about content deleted or "censored" without reason due to the Network Enforcement Act. On the other hand, the providers massively increased their German-speaking staff working in the departments for reviewing and deleting questionable postings.

Whether the Network Enforcement Act will achieve the aim of reducing hate speech and illegal content in social networks is still under review, but at least it seems to be a little step forward to maintain some minimum etiquette on social networks and to reduce the misuse of social networks for digital propaganda.

There have been discussions on additional regulatory measures not covered by the Network Enforcement Act or other laws. One proposal is an obligation to detect and label non-human contributions or contributors in social network discussions. Those so-called social bots played an important part in earlier digital propaganda campaigns by commenting, supporting, sharing, and even issuing politically extreme postings and fake news. The development of technologies to detect such bots is still in an early phase; there will never be a 100 percent correct detection rate since the creation of social media bots is ongoing. But at least such a measure can raise awareness of the fact that a lot of the supporters of a specific campaign may in fact be computer programs.

Last but not least, it should be mentioned that very severe cases of fake news may result in criminal investigation and charges. This may be the case if the assumptions are insulting or defamatory. In Germany, the incitement of the people and the denial of the Holocaust are criminal offenses, whereas those expressions may be protected by freedom of speech in the U.S.

But it is also clear that the contribution of criminal courts in the field of digital propaganda will only have minimal results since a well-planned propaganda campaign will be able to avoid crossing this line. And in the rare case that an individual may be sentenced, this bears the risk that he or she may become a martyr among his or her supporters and fuels the campaign instead of stopping it.

Cyber Threats in General

But it is not only digital propaganda jeopardizing the reliability and stability of democratic states and institutions. Governmental institutions as well as companies and society must be able to face all kinds of cyber threats posed to them by state and non-state actors. As such, the German government and the EU took several measures in the last few years.

The main legislative measure aside from the Network Enforcement Act on the European level is the Network and Information Security (NIS) Directive from 2016, which had to be transposed into national law by May 2018. It aims at establishing Computer Security Incident Response Teams (CSIRT) and National NIS Authorities in the EU member states, an EU-wide cooperation group, and a CSIRT network. It also provides security standards and obligations to notify operators of so-called essential services, including energy, transport, water, banking, financial market, and digital service providers of serious incidents.

One of the most important measures needed in light of growing cyber threats is capacity building within the competent authorities and companies. The German Federal Government already established the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) in 1991. Its main tasks in the beginning were the encryption and security of governmental communication and the certification of IT systems for the handling of restricted information. More recently, the BSI Act, which established the office, has faced two major amendments in 2009 and 2015 adding competences to protect governmental networks, develop IT security standards, and set standards for essential service providers. These regulations became the blueprint for the previously-mentioned NIS Directive). The BSI has also acted as the CERT for the federal government since 1994 and the CSIRT since 2017 and is—since 2018—the National NIS Authority in Germany.

Since 2011, the work of the BSI is complemented by the National Cyber Defense Center (Nationales Cyber-Abwehr Zentrum, CyberAZ)). This is a cooperation platform of several federal authorities (BSI, Federal Police and Federal Criminal Police, the intelligence services, the civil protection and disaster assistance, and the German armed forces) with the task of collecting information on cyber threats and cyber incidents. Its main products are situation reports and detailed warnings and recommendations concerning cyber incidents for state authorities and companies.

One of the most recent developments in the field of cyber capacity building is the Center for Information Technology in the Field of Homeland Security (Zentralstelle für Informationstechnik im Sicherheitsbereich, ZITiS), founded in 2017. It is meant to act as a center of expertise for technical questions concerning security authorities. It is doing research and development on methods, tools, and advice for security authorities, e.g., in the fields of digital forensics, lawful interception, and crypto analysis.

With technology changing and rapidly developing, the threats posed to and by information technology are developing as well. This means that policymakers and governments have to be aware of the cyber challenges and to keep their eyes on new developments to be able to react appropriately to cyber threats and digital propaganda.

A DEMOCRATIC RESPONSE TO DIGITAL DISINFORMATION

THE ROLE OF CIVIL SOCIETY

BRET SCHAFER

Numerous factors complicate efforts to combat digital disinformation, not the least of which is the near impossibility of establishing a universal set of standards that could define what is and is not “disinformation.” This taxonomic dilemma is amplified by different cultural and legal standards related to freedom of speech. Protected free speech in the United States, for example, is vastly different from freedom of expression in Germany. Unlike terrorist content or child pornography, both of which plainly and egregiously violate societal norms and, in some cases, federal and international laws, digital disinformation falls into a difficult-to-codify gray zone. Democratic governments and social media platforms are loath to regulate this space, for the justifiable and perhaps laudable fear of being seen as “arbiters of truth”—a role that is anathematic to free, open exchanges of information.

Of course, authoritarian and autocratic regimes face no such misgivings in their efforts to regulate content online. This creates an uneven playing field where the rules and norms that apply to democratic players are simultaneously ignored and exploited by undemocratic ones. Because malign foreign actors often mimic the vitriolic and polarizing messages and themes championed by certain domestic groups, it is enormously challenging to disaggregate protected speech from foreign influence operation. This is especially true in the United States, where the First Amendment provides broad cover for those who seek to hijack and manipulate public discourse. Any effort to coordinate a response to digital disinformation, whether offensive or defensive in nature, must therefore recognize that democratic societies, at least in the short term, are fundamentally more vulnerable to information operations than authoritarian ones.

While it is important to understand this imbalance, it is equally important to resist the urge to undermine freedom of speech or expression in the name of national security. Doing so would not only weaken democracy, it would validate the repressive tactics authoritarians use at home. It is therefore essential that policymakers dogmatically adhere to our values in order to avoid unintended negative externalities in the search for a “solution” to computational propaganda. This is not just a matter of principle but of strategic necessity: we cannot allow our very real need to protect the credibility of information to erode the very values that foreign influence operations seek to destroy. Put simply, we must not become our adversaries to defeat them.

Instead, governments in free societies should work within the parameters of free speech and expression to be build resiliency and create deterrents. This includes enacting sensible legislation where necessary and creating entities that can identify and respond to emerging digital threats. But unlike autocratic and authoritarian regimes that must rely on top-down solutions, democracies have the benefit of being able to employ a grassroots approach to the problem. Solutions need not come from capitals, nor do they need to be driven by heavy-handed regulation. Tech and social media companies certainly have an outsized role to play, but civil society actors in the United States and Europe can draw upon a wealth of knowledge and expertise to mitigate vulnerabilities and strengthen resolve. Independent and credible fact checkers are key, but so are technologists, educators, digital forensic analysts, and strategic communications professionals, to name but a few. Digital disinformation is not just a technological or informational problem; it is a whole-of-society problem.

Therefore, we must find whole-of-society solutions.

The Role of Civil Society

Civil society can play four primary roles in the fight against computational propaganda. First, it can act as a watchdog, policing social media and exposing disinformation campaigns as they emerge. Second, it can help to inoculate publics against information manipulation by supporting education outreach and media literacy programs. Third, it can apply pressure to tech companies, businesses, and advertisers that wittingly or unwittingly host, support, or incentivize creators of false and misleading content. Finally, civil society can work with governments, the media, and each other to improve the conditions of mistrust and polarization that create fertile breeding grounds for the spread of disinformation. In all cases, these efforts can and should expand beyond domestic borders and include like-minded groups throughout the transatlantic space. European and American democracies are bound together by common values that supersede any legal or cultural differences. Finding a unified voice and drawing upon each other's experiences and best practices is essential, not only in the fight against digital disinformation, but also in the broader context of rebuffing authoritarian threats to democracy.

CIVIL SOCIETIES' ROLE IN MONITORING, COUNTERING, AND EXPOSING DISINFORMATION

The first line of defense against digital disinformation is to expose and refute efforts to manipulate information. This involves proactive measures to raise awareness of the tactics and techniques used to place and propagate disinformation as well as reactive measures to analyze, verify, and, if necessary, debunk specific narratives. Fact-checkers are often viewed as the tip of this spear, but in reality, they are the rear guard whose work is to clean up the historical record for posterity's sake. As countless studies have shown, if a false narrative enters the public's bloodstream, it is nearly impossible to reverse the deleterious effects.[1] Therefore, we need groups out front who can identify structural weaknesses in the online information ecosystem before adversarial actors exploit them. This is a fundamental difference between traditional and computational propaganda. The former involves the manipulation of information and false narratives; the latter involves the manipulation of algorithms that can spread false narratives at an unprecedented scale and speed.[2] The response, therefore, is not just about objective truth, but also about identifying cyber vulnerabilities in the information space.

Governments can and should play a role in these efforts. The United States, NATO, and many European countries have established task forces that monitor and track disinformation campaigns, including NATO's StratCom Center of Excellence and the U.S. State Department's Global Engagement Center. These efforts are critical, particularly in instances when widespread disinformation campaigns threaten public health and safety or national security. Often, however, information operations do not reach the threshold of triggering a government response.

Additionally, in the United States, there is no single agency tasked with alerting the public to active or developing disinformation campaigns, whether online or off. The agencies most likely to spot emerging campaigns originating from abroad—the NSA, CIA, and the State Department—are either ill equipped or expressly prohibited from handling domestic outreach, leaving a gap that, at least at the moment, must be filled by civil society.

Credibility is also key. While certain European governments—most notably, those in Scandinavia and the Baltics—have proven to be adept at exposing and communicating online threats to their societies, many governments suffer from profound credibility gaps.[3] The specter of political motivations will always haunt government efforts to unmask foreign influence operations, casting doubt on the viability of government-driven fact-checking efforts. Although civil society groups are certainly not immune to real or perceived biases, they are in a better position to independently verify information, particularly if they can prove their nonpartisan or bipartisan credentials. The Poynter Center's International Fact-Checking Network and the Kyiv Mohyla Journalism School's StopFake.org are two initiatives that have proven effective at exposing disinformation in general, and, in the case of StopFake, Kremlin-generated disinformation in particular.[4]

Projects like the Alliance for Securing Democracy's Hamilton 68 dashboard, the Atlantic Council's Digital Forensic Research Lab, and the tech-savvy volunteer collective Data for Democracy have also exposed the computational tools used to amplify false narratives on social media.[5] By identifying inorganic nodes in social media networks and raising awareness of malicious automation and systemic vulnerabilities, these groups have moved the conversation away from one that focuses exclusively on narrative solutions to one that addresses broader cyber vulnerabilities. Alone, these initiatives are merely a ripple in the proverbial pond, but combined with research from the academic community, including Indiana University's Center for Complex Networks and Systems Research (cNetS), Harvard University's Belfer Center, and Columbia University's Tow Center for Digital Journalism, these efforts have slowly begun to change the strategic paradigm.[6]

Moving forward, improving coordination mechanisms between these efforts will be critical to avoid redundancies and elevate each other's work. The Atlantic Council's Disinformation Portal is a good initial step.[7] So, too, was the AICGS / HSS Transatlantic Cybersecurity Partnership, which brought together American and German academics, civil society groups, government officials, and business leaders to exchange ideas and best practices.[8]

BUILDING RESILIENCE THROUGH EDUCATION

Despite the best efforts of the fact-checkers and troll hunters, efforts to counter disinformation can only do so much. The problem is simply too vast and the tools too varied. It is thus essential that civil society work to raise awareness of the threat with the public, and to advance programs that can educate citizens so that they have the tools to protect themselves. This means that groups engaged in disinformation research must break out of the bubble of capital cities and engage publics at the local level, especially in disaffected communities that are often targeted by malign influence operations.

Media literacy is one solution, but it is not a silver bullet. This is especially true with efforts to reach older generations, who may have the necessary critical thinking skills but lack familiarity with digital concepts like filter bubbles, fake online personae, or malicious automation. Traditional education outreach through schools will obviously miss this portion of the population. Regardless of the limitations, however, there is a clear need for local civil society groups to train educators and students about how to detect information operations online, and how to be responsible and critical consumers of news. This is especially true in the United States, where the fragmented education system makes any state-driven effort nearly impossible to implement. While Europe has more buy-in at the state level and a more centralized approach to education, there is still a need there for NGOs to partner with governments to develop comprehensive media literacy programs.[9]

In addition, media literacy cannot exist in a vacuum. It must be coupled with civics education and efforts to improve civic participation. The foundation of most conspiracy theories is a distrust of government and a sense of removal from the political process. Efforts to explain how democratic governments function and how citizens can be more engaged in the democratic process will shatter many disinformation narratives.

Finally, civil society should work to support local and independent media. This not only involves direct support for journalists working in underserved communities or covering under-covered topics, but also efforts to inform journalists about how to protect themselves from malign foreign influence. This includes pushing for standards in how the journalistic community responds to leaks of hacked information, as well as best practices for verifying social media accounts are legitimate before using them as sources in a story.[10]

APPLYING PRESSURE WHEN AND WHERE NEEDED

Citizens in democratic countries have the power to demand that elected officials take the threat of digital disinformation seriously. As consumers, they also have the ability to apply pressure to the platforms and services that have facilitated the spread of disinformation. Civil society groups can fight this battle on multiple fronts, from direct engagement with companies to public name-and-shame campaigns. If needed, they also have the power to organize boycotts and to pressure advertisers to end relationships with companies that wittingly or unwittingly facilitate the spread of disinformation.

It is important to recognize that many creators and distributors of computational propaganda have non-ideological motivations. From Macedonian fake news factories to celebrity follower factories and corporate trolls-for-hire, there is an entire online economy devoted to the manipulation of information.[11] While many of these for-profit services are used for relatively benign purposes (for example, the posting of inflated product reviews on Amazon or the artificial amplification of views on YouTube), almost all can be abused in more malicious ways. The significant overlap between profit-driven and ideological manipulators of information thus requires that civil society groups target the entire digital disinformation ecosystem, not just the tentacles that connect directly back to malign state or non-state actors.

In fact, civil society would be wise to focus its efforts on exposing and degrading for-profit disinformation efforts rather than those operated by ideological extremists or hostile state governments. On the surface, this approach may seem counter-intuitive; after all, why go after the small arms dealers rather than the armies? But degrading the profitability of these commercial disinformation ventures would shrink the community of bad actors online, leaving only the “true believers” and those directly financed by authoritarian governments or extremist groups. This not only would make efforts to expose misleading content more manageable, but it would also limit the ancillary tools and services available to those engaged in large-scale information operations.

A critical cog in the for-profit disinformation wheel is online advertising. Often, however, companies are completely unaware that their brands are appearing on questionable sites. Because major brands enlist third party ad tech companies to place their ads online, the decision to place ads on specific sites is made by an algorithm rather than by an image-conscience brand director. This differs from television, radio, and print ad buys, where advertisers are acutely aware of the content that is associated with their brands. For obvious reasons, reputable companies do not want their brands associated with sites that peddle hyper-partisan or factually questionable content. Drawing attention to instances when ads for reputable companies appear on less-than-reputable sites is an effective tool in applying pressure up the food chain. The potential loss of a significant revenue stream often carries more weight than the threat of legislation.

ADDRESSING THE ROOT CAUSES

Disinformation is only effective if the target audience is receptive. Influence is not mind control: it is a nudge or a shove, usually in the direction someone is already predisposed to lean.[12] No amount of disinformation can change hardened views, but a targeted campaign can push a targeted population—whether on the far left or the far right—to an even more radicalized position. It can inspire people to action, but it can also drive people to inaction. In a democracy, both results are highly problematic.

Civil society must therefore work to address people’s core grievances with democracy and the liberal international order. The wave of populism that has swept across Europe and the United States did not result from digital disinformation; it resulted from very legitimate concerns. Those engaged in the fight against computational propaganda would be wise to keep those concerns in mind, and to avoid rhetoric that risks further alienating certain populations. Ultimately, the best defense against digital disinformation is to address the real-world issues that disinformation seeks to exploit.

NOTES

[1] Elizabeth Kolbert, “Why Facts Don’t Change Our Minds,” *The New Yorker*, 27 February 2017.

[2] Renee Diresta and Jonathon Morgan, “Information Operations are a Cybersecurity Problem: Toward a New Strategic Paradigm to Combat Disinformation,” *Just Security*, 10 July 2018.

[3] Christian Caryl, “If You Want to See Russian Information Warfare at its Worst, Visit these Countries,” *The Washington Post*, 5 April 2017. Online.

[4] See https://www.poynter.org/channels/fact-checking and https://www.stopfake.org/.

[5] See http://dashboard.securingdemocracy.org/, https://medium.com/dfrlab, and http://datafordemocracy.org/.

[6] See http://cnets.indiana.edu/, http://datafordemocracy.org/, and https://towcenter.org/.

[7] See https://disinfoportal.org/.

[8] See https://www.aicgs.org/project/transatlantic-cybersecurity-partnership/.

[9] Jamie Fly, et al., “Policy Blueprint for Countering Authoritarian Interference in Democracies,” Alliance for Securing Democracy, 26 June 2018, pp. 34-35. Online.

[10] Heidi Tworek, “Responsible Reporting in an Age of Irresponsible Information,” Alliance for Securing Democracy, 23 March 2018. Online.

[11] Samantha Subramanian, “Welcome to Veles, Macedonia: Fake News Factory to the World,” *Wired*, 15 February 2017. Online; Nicholas Confessore, et al., “The Follower Factory,” *The New York Times*, 27 January 2018. Online; and Elizabeth Dwoskin and Craig Timberg, “How Merchants use Facebook to Flood Amazon with Fake Reviews,” *The Washington Post*, 23 April 2018. Online.

[12] Bret Schafer and Andrew Weisburd, “Insinuation and Influence: How the Kremlin Targets Americans Online,” Alliance for Securing Democracy, 16 October 2016. Online.

Left
Cyberwarfare specialists serving with the 175th Cyberspace Operations Group of the Maryland Air National Guard engage in weekend training at Warfield Air National Guard Base, Middle River, Md., June 3, 2017. Navy Adm. Michael S. Rogers, director of the National Security Agency, commander of U.S. Cyber Command, and chief of the Central Security Service, briefed the Senate Armed Services Committee on Cyber Command's role in the support of the nation's defense against its adversaries, Feb. 27, 2018. U.S. Air Force photo by J.M. Eddins Jr.
VIRIN: 170603-F-LW859-023.JPG
https://www.defense.gov/Photos/Photo-Gallery/igphoto/2001883314/

Right
Real-time cyberattacks, including information on the attack's origin, type, and target, as well as the attacker's IP address, geographic location, and ports being utilized, are displayed on the Norse attack map on the 275th Cyberspace Squadron's operations floor, known as the Hunter's Den. The squadron is one of four squadrons compromising the 175th Cyberspace Operations Group of the Maryland Air National Guard at Warfield Air National Guard Base, Middle River, Md., Dec. 2, 2017. U.S. Air Force photo by J.M. Eddins Jr.
20171202-F-LW859-013' CC 2.0
https://www.flickr.com/photos/airmanmagazine/40080902694

Original Article: J.M. Eddins Jr. "Citizen Cyber: Air Guard built for rapid change of digital battlespace." Airman Magazine, March 13, 2018, http://airman.dodlive.mil/2018/03/13/citizen-cyber/

The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

American Institute
for Contemporary
German Studies

JOHNS HOPKINS UNIVERSITY