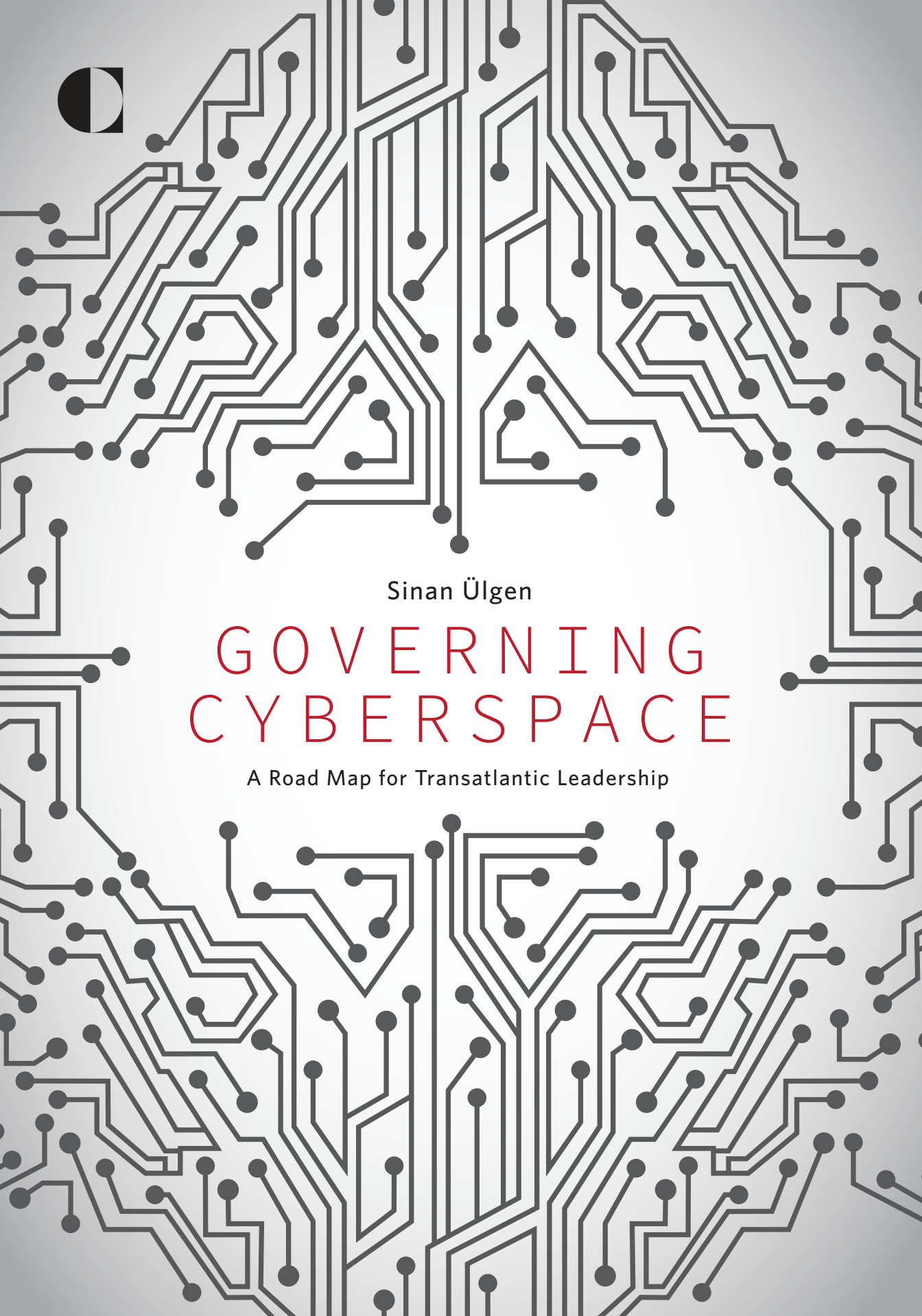

Sinan Ülgen

GOVERNING CYBERSPACE

A Road Map for Transatlantic Leadership

Sinan Ülgen

GOVERNING CYBERSPACE

A Road Map for Transatlantic Leadership

CARNEGIE EUROPE

Carnegie Europe is grateful to Microsoft for its support of this publication.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue, NW
Washington, DC 20036
P: +1 202 483 7600
F: +1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org/pubs.

TABLE OF CONTENTS

ABOUT THE AUTHOR

Sinan Ülgen is a visiting scholar at Carnegie Europe in Brussels, where his research focuses on the implications of Turkish foreign policy for Europe and the United States, nuclear policy, and the security and economic aspects of the transatlantic relations. He is a founding partner of Istanbul Economics, a Turkish consulting firm that specializes in public and regulatory affairs, and chairman of the Center for Economics and Foreign Policy Studies, an independent think tank in Istanbul.

Ülgen is a regular contributor to Turkish dailies, and his opinion pieces have been published in the *International New York Times*, the *Financial Times*, the *Wall Street Journal*, *European Voice*, and *Le Figaro*. He was a member of the international security experts group set up by former NATO secretary general Anders Fogh Rasmussen and tasked with preparing a report on the transatlantic relationship in advance of NATO's September 2014 summit. He is the author of *The European Transformation of Modern Turkey With Kemal Derviş* (Center for European Policy Studies, 2004) and *Handbook of EU Negotiations* (Bilgi University Press, 2005).

***

The author would like to thank Grace Kim, research assistant at the Center for Economics and Foreign Policy Studies (EDAM), for her valuable assistance during the preparation of this report.

SUMMARY

Cybertechnologies are rapidly changing the international landscape, but leaders in government, business, and elsewhere are just beginning to understand the ramifications, both good and bad, of an interconnected digital world. Weak international governance of cyberspace stands in stark contrast to the accelerating pace of challenges. To shape the regimes that govern cyberspace to the advantage of generations to come, the United States and the European Union should forge a joint policy vision.

THE ROLE OF THE TRANSATLANTIC PARTNERS

- Given their economic and technological edge, the United States and Europe have a natural interest in playing a more influential role in the cybernorms debate.
- Washington and Brussels have started to engage third countries on cyberpolicy issues to develop multilateral norms. The impact of these disparate attempts can be greatly enhanced by a transatlantic effort to identify and jointly shape a more ambitious global agenda.
- The feasibility of any joint initiative will depend on the potential for convergence between Washington and Brussels on key policy areas related to cyberspace, such as online privacy, Internet freedoms and governance, cybersecurity, and cyberwarfare.

- There is a significant degree of real and potential convergence between the transatlantic partners, and these areas should provide the basis for a new approach to creating a global policy framework for cyberspace.

HOW TO CAPITALIZE ON AREAS OF CONVERGENCE

Develop norms regulating government-industry collaboration on mass data collection and retrieval. To enhance trust in the Internet, the transatlantic partners should develop a joint code of conduct for regulating interactions between government agencies, large Internet companies, and data handlers regarding access to online data.

Create a new multilateral instrument to prevent cybercrime. The transatlantic partners should develop more robust ways to detect and analyze cyberattacks so that culprits can be more easily identified and future attacks better deterred.

Propose amendments to international trade law to introduce penalties for economic cyberespionage. Changing World Trade Organization rules will require a joint action led by the transatlantic partners.

Lead efforts to codify norms governing the export of surveillance technologies. The transatlantic partners should guide this effort that would help to constrain the capacity of illiberal regimes to restrict Internet freedoms.

Agree on a mandate for NATO to develop a more robust approach to cyberdeterrence. The North Atlantic Treaty Organization has developed a strategy focused on enhancing the resilience of the alliance against cyberattacks. But NATO also needs a more offensive posture to improve its overall deterrence.

INTRODUCTION

King Philip VI of France was an unlucky man. In one of the key battles of the Hundred Years' War in 1346, he led a French army hoping to rout a smaller contingent of English forces. Entering the theater of war, he did not know that the Battle of Crécy would later become famous for the first use of gunpowder on a European battlefield. This tactical advantage allowed the English to score a decisive victory over the French and paved the way for future English triumphs. The discovery and wider adoption of gunpowder would not only change the nature of battle in the Middle Ages but also gradually lead to the upending of the medieval social order. Suddenly, a military and social structure organized around an impregnable fortress and an associated hierarchy of castes looked much more vulnerable.

Advances in the world of digital interconnectedness have many of the attributes of the quintessential disruptive technology that gunpowder exemplifies, with the fundamental difference that the changes brought about by the omnipresence of cybertechnologies are happening at an exponential pace. But this is not merely a technological revolution. Combined with the undercurrent of globalization, the emergence of a digital world is upending the old order. The vast opportunities that this brings have had a revolutionary impact on a range of issues, from the way countries are ruled to the way economies are managed. But just as this burgeoning cyberreality has contributed to a positive global agenda presenting prospects for more inclusive, accountable democracies and more equitable, sustainable

increases in incomes, it has also brought to the fore a darker agenda of state surveillance and repression, security threats, wide-scale espionage, and even doomsday scenarios.

In a sense, current thinking about the cyberworld is very similar to the early days of the nuclear age, when mankind had to come to terms with an astonishingly powerful technology that could either protect peace or annihilate civilization. The dilemmas facing today's leaders for the governance of the cyberworld are perhaps not as drastic, but they are still enormously complex.

This report is an effort to explore the novel and specific international policy challenges created by the emergence of this multifaceted cyberspace. This includes the policy implications of online privacy and national security, data confidentiality, cross-border data flows, freedom of expression online, Internet governance, Internet taxation, cybersecurity, and cyberwar. An aim is to clarify the global policy challenges created by the emergence of a cyberworld, so each chapter starts by outlining the implications of a lack of multilateral governance for the Internet. The positions of a few lead countries—the United States, the European Union (EU), Russia, and China—on key cyberpolicy questions are covered. And other countries that have developed particular narratives in specific cyberpolicy areas, like Brazil and India on the management of the Internet or Iran on Internet freedoms, are included as well. Taking into account the configuration of current efforts to develop and codify norms for cyberspace, a road map for transatlantic leadership emerges. There is a realistic and much-needed common agenda for Washington and Brussels to influence the development of global norms for cyberspace.

CHAPTER ONE

PRIVACY ON THE INTERNET

When the *Guardian* was engaged in internal discussions about whether or not to publish the thousands of files stolen by former U.S. National Security Agency (NSA) contractor Edward Snowden, the U.S. government asked the British newspaper to refrain from printing the story, saying "foreign enemies would switch to new forms of communication and make it harder for the NSA to break."[1] Despite attempts at dissuasion, the *Guardian* decided in June 2013 to run the story because the scale of the surveillance programs warranted "public debate regarding government actions that weaken the most powerful tools for protecting the privacy of Americans and others," a sentiment Snowden has repeatedly echoed during interviews when asked about his motivation for leaking the files. In response, British government officials entered the *Guardian*'s offices and destroyed hard drives containing leaked information.

The June 2013 leaks have left in their wake a trail of political uproar and public outcry against the broad-sweeping powers given to governments in the name of national security. The uncovering of what the European Parliament called a "reconfiguration of surveillance that enables access to a much larger scale of data than telecommunications surveillance of the past" and the controversy that followed these revelations have forced not just the United States but also other governments to reexamine their own privacy and security policies and balance the will of their people with the safety of their countries.[2]

Diverse political, judicial, and cultural traditions shape countries' positions in the debate on privacy versus security. Every country has a different set of political and economic incentives to consider when pursuing its national interests. At the crux of the debate today are the same political, historical, and social factors that underpin the age-old question of the extent to which a government can curtail individual rights in the name of national security.

This debate has been rekindled not only by the public disclosure of the scale and scope of ongoing surveillance by intelligence agencies but also by the changing overall dynamics of the digital world. The globe is increasingly awash with data, including personal information. The proliferation of activities that generate personally identifiable data, from cell phone usage to digital payments and from the use of location-based services to Internet searches, has led to a multiplication of platforms for data extraction. Coupled with enhanced and more cost-effective technologies for electronic surveillance, these changes have vastly increased the opportunities for governments to identify, seize, store, and analyze personal data.

The advent of the Internet of Things, a network designed to boost the interconnectivity of key objects and appliances from cars to homes, will add another layer of complexity. As emphasized in a statement by the Global Commission on Internet Governance, which researches Internet-related dimensions of global public policy, "everything we do, see, use or touch will leave electronic tracks, enlarging further both the potential commercial and social value of such data. It also will expand the opportunities provided for police and intelligence agencies to learn more about their suspects."[3]

But beyond the question of how much leeway governments should be given to collect data about their citizens on the web, the contours of the public-private partnership that has emerged in this sphere remain nebulous. Today, Internet giants like Google and Facebook can access and aggregate more data than many governments can, making these companies both targets of cyberintrusion by hackers and central elements of some large-scale government programs to collect personal data. In an op-ed for the *Financial Times*, Robert Hannigan, the current director of the United Kingdom's Government Communications Headquarters, a government intelligence and security organization, stated that British intelligence could not tackle the challenge of extremism without greater support from the private sector, including the largest U.S. technology companies that dominate the web. "However much [these companies] may dislike it, they have become the command-and-control networks of choice for terrorists and criminals, who find their services as transformational as the rest of us," he wrote.[4] Therefore, these companies have an ever-increasing responsibility to

The contours of the public-private partnership that has emerged in the digital sphere remain nebulous.

demonstrate to their client base the integrity of their policies and procedures and to better protect their customers' private information.

A more divisive aspect of the global discussion on Internet privacy concerns policies on encryption. This debate was revived by the attacks perpetrated by the self-proclaimed Islamic State in Paris in November 2015, when terrorists allegedly communicated by way of encrypted messaging services like WhatsApp and Apple's iMessage. Government authorities see encryption technologies as a serious barrier to their efforts to monitor the communications of radical and terrorist entities. Governments have therefore been pushing global Internet companies to allow intelligence services to use a backdoor to access encrypted messaging platforms as well as the contents of smartphones. Privacy advocates argue that such backdoors would substantially weaken online privacy, as they can also be exploited by hacker groups. Apple's Chief Executive Officer Tim Cook warned that "any back door is a back door for everyone."[5]

POLICY POSITIONS

There is a clear split between liberal Western democracies and authoritarian regimes, such as China and Russia, over the right balance between security and online privacy. In the West, the debate regarding digital privacy has shifted, especially in the wake of the Snowden affair, from a question of a balance between data protection and national security to one of collective freedoms and democracy. Differences remain between U.S. and European approaches to Internet privacy, and questions of accountability regarding the scope of activities of the myriad U.S. intelligence agencies are still unanswered—at least to the satisfaction of European governments.[6] Yet even in Europe, the Islamic State's actions in France may swing the pendulum toward security. For the likes of China and Russia, national security objectives clearly outweigh privacy concerns.

United States

Reflecting the strong guarantees of the protection of privacy enshrined in the U.S. Constitution and the Fourth Amendment, the Electronic Communications Privacy Act of 1986 limited the ability of U.S. law enforcement authorities to access private communications. The act also penalized the disclosure of illegally obtained information. But the U.S. government's reaction to the terrorist attacks of September 11, 2001, led to a rebalancing of the privacy-security outlook, with scaled-up government surveillance efforts that have increasingly invaded the privacy of citizens in the name of national security. For example, the Patriot Act of 2001 expanded investigative methods to enhance government agencies' access to online data.

Snowden's uncovering in June 2013 of the NSA's largest domestic surveillance programs in its history—including the exploitation of private data links, the wiretapping of phone

calls, and sometimes even the strong-arming of Internet companies to siphon off private data—fundamentally changed the way the public talks about the debate over privacy versus security.

The United States was forced to review its approach to privacy on the Internet as the global and domestic reactions to the Snowden revelations took shape. When Germany learned of alleged U.S. wiretapping of Chancellor Angela Merkel's cell phone, it asked for the repatriation of the U.S. Central Intelligence Agency (CIA) station chief in Berlin and publicly denounced the U.S. government's violation of privacy rights. Although Germany later dropped its investigation into the wiretapping claims due to a lack of evidence, the rift caused by the revelations continues to shape the public debate about surveillance programs.

These reactions have not been limited to the political domain but have also affected U.S. commercial interests as other countries have become wary of purchasing U.S. goods and technical services because of privacy concerns. Total economic losses to American companies between 2013 and 2016 have been estimated to range from $22 billion to $180 billion.[7] Anecdotal evidence has also pointed to "increased reluctance on the part of non-US businesses to entrust data to US cloud services and other [information and communications technology] providers," in the words of Cameron Kerry of the Brookings Institution.[8]

U.S. President Barack Obama signaled a shift in the approach of his administration in January 2014 with a policy directive that "made explicit and binding the limits that the United States places on foreign intelligence collection."[9] To consolidate this more privacy-focused approach, the Big Data and Privacy Working Group led by former counselor to the president John Podesta recommended that protections of personal information under the 1974 Privacy Act apply regardless of a person's nationality.[10] U.S. government officials have also begun to take steps to repair the broken trust between private companies and the government. Obama and U.S. Secretary of Defense Ashton Carter have met with technology leaders in Silicon Valley to muster support for public-private partnerships.

European Union

The EU's Lisbon Treaty, which came into force in 2009 with the aim of making the union more efficient, set out data protection as a fundamental right. As a result, the EU and its member states have tended to prioritize privacy over security. The EU's Charter of Fundamental Rights also specifically protects the rights to privacy, data protection, and effective judicial remedy. Data privacy is regulated in the EU by the 1995 Data Protection Directive.

In 2012, the European Commission proposed a new and updated framework with the General Data Protection Regulation, with a view to unifying the different regimes of EU member states while adding significant new regulatory requirements. The regulation sets out new rules for the commercial collection and use of personal data and enhances data confidentiality. Clarifying the aims of the EU's renewed approach to data privacy, Viviane

Reding, then the European commissioner for justice, fundamental rights, and citizenship, underlined the four essential components of the proposed European data protection system.[11] Reding emphasized that

> the territorial scope of regulations should be clearly and expansively defined such that non-European companies must be required to comply fully with European rules. Second, the concept of personal data should be expanded to include not only the content of e-mails and telephone calls but also traffic data pertaining to that content. Third, these rules should apply not only to companies that collect data from citizens, but also to companies that process data such as cloud providers. Finally, there must be protection against unrestricted international data transfers. Data of EU citizens should be given to non-European law enforcement agencies only under clearly defined and exceptional circumstances and only if subject to judicial review.[12]

Beyond EU legislation, European governments' programs of Internet surveillance have also been constrained by the extension of human rights norms to the digital universe. The role of the European Court of Human Rights, the tribunal of the Council of Europe, as the ultimate adjudicator of the European Convention of Human Rights has been instrumental in this regard. A landmark decision was the court's judgment in the 2006 case of Weber and Saravia v. Germany.[13] The court was asked to examine the legality of the telecommunications recording carried out by the German Federal Intelligence Service. In its ruling, the court accepted the German government's claim that interference with the secrecy of telecommunications was necessary in a democratic society in the interests of national security and for the prevention of crime, and that German legislation provided adequate and effective guarantees against abuses of the state's surveillance powers. More importantly, the court established in the Weber case a set of criteria for determining the lawfulness of secret surveillance to avoid the abuse of powers and arbitrariness.[14] While underlining that the risks of arbitrariness are particularly evident in those cases in which an executive power is exercised in secret, the court held that "the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."[15]

European governments' programs of Internet surveillance have been constrained by the extension of human rights norms to the digital universe.

Russia

The Russian Federation's priority is its security, which often trumps privacy concerns raised by citizens. Russia under President Vladimir Putin has concentrated most decision-making power at the top of the government, allowing for better and quicker control of

censorship and Internet policy. The Federal Security Service (FSB), the main successor of the Soviet Committee of State Security (KGB), is Russia's internal security agency. The FSB oversees Russia's antiterrorism, counterintelligence, electronic intelligence, crime investigation, and border control activities, often involving multiple agencies and government organizations in its efforts.

The FSB may legally intercept all electronic communications under the System of Operative-Investigative Measures (SORM), a program started in the 1980s during the Cold War and continuously upgraded ever since to serve the interests of the Kremlin. The FSB obtains court orders to eavesdrop on domestic and foreign nationals—although it is questionable how stringently judges scrutinize the justifications for the orders. However, the service is not required to show its warrants, specify its targets, or share retrieved information with the telecommunications companies and Internet service providers (ISPs) from which the service siphons off data. Unlike the NSA, which has to obtain a court order for every information request, once the FSB obtains a warrant, it has free rein to access companies' servers without obtaining additional orders. Moreover, network operators and ISPs are required to purchase and install SORM equipment themselves without having access to the surveillance boxes that store their data. According to an article in the *World Policy Journal*, "The FSB has control centers connected directly to operators' computer servers. . . . In every Russian town, there are protected underground cables, which connect the local FSB bureau with all Internet Service Providers . . . and telecom providers in the region."[16]

China

China openly prioritizes security over privacy, and the country's highly centralized political system and proclaimed principle of cybersovereignty provide the legal justification to monitor, regulate, and censor online content that threatens the political stability of the regime. As stated by China Radio International, Chinese President Xi Jinping's conception of cybersovereignty "has two levels of significance: an internal component where each government has the right to develop, regulate, and manage its domestic Internet in line with its national independent autonomy; and an external component involving the right to defend its Internet from foreign intrusion and attack."[17] Chinese government surveillance has long been the established norm in China, but the growing influence of Western Internet companies in the country will continue to be a major point of contention in balancing China's national security priorities with privacy rights championed by foreign firms.

China's emphasis on maintaining control over content on the Internet also extends to control over Internet access and technology. An extension of the principle of cybersovereignty, importing Internet technology products is conditioned on China's suppliers agreeing to adhere to China's laws and regulations. As long as businesses follow Chinese rules, they can tap into the country's population of over 1 billion potential customers.

In recent years, however, China has taken bolder steps to ban foreign-made hardware and services outright and has continued to exert more pressure on non-Chinese companies to conform to Chinese cyberstandards. Beijing joined the rest of the world in lambasting U.S. surveillance programs following the Snowden leaks in June 2013, providing the opportunity for China to pass protectionist legislation to foster growth in its domestic technology industry under the pretense of antisurveillance and national security laws. According to Reuters, from 2012 to 2014, "The number of approved foreign tech brands fell by a third," and more Chinese-made products were approved.[18] In May 2015, the Communist Party of China even discussed a counterterrorism law "that would require many companies operating within China and foreign firms supplying software to China to hand over source code to authorities and use Beijing-approved encryption methods," according to the *Hill*.[19] Top government officials often cite the Islamist and separatist threat from the mainly Muslim region of Xinjiang in far-western China as the impetus for tougher antiterrorism laws. However, the extremist threat from Xinjiang fails to convincingly explain how laws banning the use of the Microsoft Windows 8 operating system on government computers will make the country safer.

POLICY INITIATIVES

A binding multilateral set of norms establishing a globally accepted balance between privacy and security concerns is not to be expected. Differences in political, social, and cultural legacies are just too significant and unbridgeable for governments to realistically aim for this lofty goal. However, the Snowden revelations and the enormity of U.S. surveillance, with its global reach, have rekindled interest in the quest for such universal standards.

A binding multilateral set of norms establishing a globally accepted balance between privacy and security concerns is not to be expected.

The United Nations (UN) undertook a key effort in this area in December 2013 when the General Assembly adopted by consensus a resolution, which had been introduced jointly by Brazil and Germany and co-sponsored by 57 member states, on the right to privacy in the digital age. The resolution framed Internet privacy in the context of human rights and called "upon all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data, emphasizing the need for States to ensure the full and effective implementation of their obligations under international human rights law."[20] The resolution also requested that the UN high commissioner for human rights prepare a report on the protection and promotion of the right to digital privacy.

The high commissioner's report, published in June 2014, set out a useful frame of reference for thinking about the privacy-security nexus in the digital universe.[21] First of all, the report confirmed that governments can engage in intrusive surveillance provided such activities serve a legitimate aim, have been adopted on the basis of an accessible legal regime, and are both necessary and proportionate to the specific risk being addressed. As a result, mass surveillance programs that are ostensibly part of surveillance efforts of even many Western governments can be considered violations of privacy and human rights norms. A European Parliament study underlined the same challenge, stating more emphatically that "it is the purpose and the scale of surveillance that are precisely at the core of what differentiates democratic regimes from police states."[22]

The UN report also addressed the role of businesses in relation to large-scale surveillance programs. It underlined that "mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate."[23] The report warned against state efforts to force companies to facilitate access to their networks for easier government surveillance.

Reflecting a similar approach, the Organization for Economic Cooperation and Development (OECD) has adopted its own privacy guidelines.[24] These guidelines emphasized that exceptions to the listed recommendations, including those relating to national sovereignty, national security, and public policy, should be as few as possible in number and be made known to the public.

INDUSTRY-LED INITIATIVES

Aside from intergovernmental efforts, industry, which has inevitably been drawn into the discussion of how to better ensure online privacy, has striven to set up a number of different platforms to develop a common stance. In general, Internet companies have launched public campaigns and sought legislative changes that increase transparency and better protect the privacy of their customers.

The Global Network Initiative (GNI) was an early effort to establish privacy norms and codes of conduct for the ways in which companies should respond to government requests for information. Launched in 2008 as a coalition of nonprofit organizations, universities, and financial institutions with the backing of Google, Yahoo, and Microsoft, the GNI brings together members that commit to "collaborate in the advancement of user rights to freedom of expression and privacy."[25] The initiative's other aim is to facilitate the emergence of a common approach to protecting online privacy. But the GNI's effectiveness and outreach has been hindered by a lack of deeper corporate participation due to

companies' fear of being perceived in third-world markets as parts of "an organization for promoting American values."[26] The GNI's standing has been marred by allegations that member companies have cooperated extensively with the NSA on its global surveillance program. A founding member of the initiative, the nonprofit Electronic Frontier Foundation, quit the grouping in 2013, citing a fundamental breakdown in confidence. Yet the GNI remains a well-suited platform to advance a more collaborative and rules-based agenda for protecting online freedoms. The initiative's impact and role could be improved with more visible support from European companies as part of a transatlantic effort to define the terms of a new cyberpolicy partnership in the post-Snowden era.

Six months after the Snowden leaks, in December 2013, eight technology companies mounted an online campaign to set new limits on government surveillance.[27] Led by Google and Microsoft, the group, also consisting of Apple, Yahoo, Facebook, Twitter, AOL, and LinkedIn, jointly launched a campaign to pressure governments—primarily the U.S. administration—to reform their online surveillance practices. The companies asked for the establishment of new principles for mass data retrieval by government agencies that would include "limiting governments' authority to collect users' information, setting up a legal system of oversight and accountability for that authority, allowing the companies to publish the number and nature of the demands for data, ensuring that users' online data can be stored in different countries and establishing a framework to govern data requests between countries."[28]

Led by the civil society groups Privacy International, Access, and the Electronic Frontier Foundation, the 2013 International Principles on the Application of Human Rights to Communications Surveillance called on states to apply international human rights law to the current digital environment. The adopted principles included "legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation, safeguards against illegitimate access, and the right to effective remedy."[29]

In April 2015, the Global Commission on Internet Governance proposed a social contract for digital privacy and security.[30] The commission recalled that online surveillance and data collection should be limited to "purposes that are openly specified in advance, authorized by law . . . and consistent with the principles of necessity and proportionality."[31] It further recommended that "laws should be publicly accessible, clear, precise, comprehensive and nondiscriminatory, openly arrived at and transparent to individuals and businesses. Robust, independent mechanisms should be in place to ensure accountability and respect for rights. Abuses should be amenable to appropriate redress, with access to an effective remedy provided to individuals whose right to privacy has been violated by unlawful or arbitrary surveillance."[32]

The Ranking Digital Rights index launched in November 2015 aims to increase transparency about the level of commitment of global Internet and telecommunications firms to the protection of Internet freedoms and online privacy.[33] Sixteen Internet and telecommunications companies were evaluated according to 31 indicators focused on corporate disclosure of policies and practices that affect users' freedom of expression and privacy.[34]

A strategy disclosed by Microsoft may foreshadow the nature of future industry responses to the unsettled transatlantic debate on surveillance and online privacy. In November 2015, the U.S. company announced a plan to better protect the privacy of its European-origin customer data from the wide-scale monitoring efforts of U.S. government agencies. The plan involves structural cooperation with the German telecommunications group Deutsche Telekom. The German company's servers will be used to store the data of Microsoft's European client base. In addition, the German group will act as the trustee of the facilities. "The companies believe this arrangement means Microsoft will not have to respond to governmental demands for information held in these data centres, forcing official requests to go through German authorities instead," according to the *Financial Times*.[35]

TRANSATLANTIC ROAD MAP

The NSA controversy has exposed the differences between the transatlantic partners over the proper relationship between security and freedom and over the legitimacy of online surveillance. The transatlantic divide remains significant despite the overlap provided by the UK's participation in the Five Eyes initiative, which assembles five like-minded countries—Australia, Canada, New Zealand, the UK, and the United States—for closer intelligence sharing and cooperation.

As the self-professed leaders of the global liberal order, the United States and the EU shoulder a unique responsibility.

It may well be that these differences are unbridgeable. The nonalignment of national security considerations in overall policymaking could preclude a real transatlantic convergence on online privacy strategies. But at the same time, as the self-professed leaders of the global liberal order, the United States and the EU shoulder a unique responsibility for devising a mutually accepted vision of a free and open society in which privacy is respected. The lack of such a reference framework not only creates political tensions but is also a hindrance to the development of more creative economic models that can leverage the resources of an interconnected world.

It is worth underlining that despite their differences, the United States and the EU were successful in concluding an agreement in September 2015 on the exchange of online data for law enforcement. The umbrella agreement incorporated stronger data protection safe-

guards to mirror the EU's higher level of data privacy standards and a right of legal redress in the case of unlawful access.

Indeed, prevailing differences over the right balance of online confidentiality and surveillance will necessarily downscale the level of ambition for a shared agenda to advance online privacy. But real progress can still be achieved—first by delineating critical aspects of the relationship between governments and large data handlers such as Internet, social media, or telecommunications companies, and second by empowering the UN as a platform to advance global norms on data confidentiality.

The United States and the EU could seek to streamline the norms of collaboration between government and industry for access to online data. The transatlantic partners can start by developing a joint code of conduct for regulating the interaction of government agencies with large Internet companies and data handlers for the purpose of mass data collection and retrieval. Brussels and Washington could, for instance, follow up on the December 2013 industry initiative led by Google and Microsoft. An element of this framework could be the elaboration of a digital due process to standardize—to the extent possible—government requests for content removal and the sharing of user data.[36]

A further component of this set of principles could be a joint commitment by the United States and EU member states not to force third parties to create backdoors as part of their software or platforms to allow government access to data.[37] The politics of such a joint effort would arguably be facilitated by some recent jurisprudence on both sides of the Atlantic that has tended to restrict the ability of government to undertake untargeted mass surveillance. The EU's European Court of Justice (ECJ) ruled in April 2014 that mandatory data retention is contrary to EU law,[38] while the New York Appeals Court found in May 2015 that the NSA's bulk collection of phone data was illegal.[39]

Moreover, provided that the transatlantic partners can foster a common approach on these salient issues, they may be more willing to jointly spearhead a global effort to adopt an international instrument requiring intelligence activities to respect data protection standards. As suggested by the European Data Protection Supervisor, the UN could be the right forum for this initiative on the basis of the International Covenant on Civil and Political Rights.[40]

Finally, the UN can be asked to lead an effort to share best practices concerning the institutional oversight of surveillance practices. In liberal democracies in which judicial independence is ensured, the question of oversight is easily resolved by assigning a special role to the judiciary for the monitoring of surveillance. But in other jurisdictions where problems related to the independence and impartiality of the judiciary remain entrenched, alternative institutional setups can be envisaged, such as the creation of public interest advocacy positions or mixed models of administrative, judicial, and parliamentary oversight.

CHAPTER TWO

FREEDOM OF EXPRESSION ONLINE

The virtual world defies the traditional boundaries of free expression, creating new problems that have yet to be resolved. The ubiquity of social media has raised questions about how existing legal norms and practices translate into ever-expanding online territories. Multiple questions and conflicts have made it difficult to conceptualize a predictable and transparent regime that protects online freedoms.

Internet and social media companies, such as Google, Microsoft, Facebook, and Twitter, wield much influence over the availability, regulation, and dissemination of information online. And although Internet-based social platforms have greatly enhanced information sharing, they have also created conflict among the companies that offer services, the consumers that use those services, and the countries in which companies and consumers are located.

These conflicts over the regulation of content stem partly from the global nature of the Internet, which transcends national boundaries. A single national or institutional entity does not control the Internet, and there are a multiplicity of jurisdictions that affect the operations of global Internet companies carrying a multiverse of content. These firms are confronted with a myriad of different national interpretations of free speech that differ from those in the companies' home countries.

The management of Internet content is ultimately the prerogative of the companies that own the online platforms. Yet, because firms like Facebook and Twitter have users of

many nationalities uploading and sharing information from all over the world to other users in countries with all kinds of political, legal, and judicial systems, the task of creating and implementing a uniform content regulation policy has proved troublesome.

An equally important factor is the lack of uniformity and transparency among global online content aggregators—the giants of social media—in terms of their content regulation practices. After being highly scrutinized over the years, these Internet companies have taken steps to explicitly outline their policies regarding content regulation and removal, but in practice, the application of these guidelines has been inconsistent and nontransparent. Internet firms' content regulation and removal policies venture into territory normally reserved for the courts.

What is more, the sheer volume of content being exchanged over the Internet makes it nearly impossible to completely control material available online. A Google spokesperson confirmed in November 2015 that over four hundred hours of video were being uploaded to YouTube every minute.[41] Companies are struggling to keep up with this rapid pace of change and content creation.

Regulating the freedom of expression online has become one of the most contentious points of debate for both the public and private sectors.

In light of these complexities, regulating the freedom of expression online has become one of the most contentious points of debate for both the public and private sectors, often pitting the owners of online platforms against the countries in which they operate. These unresolved differences highlight the need to develop a consistent policy that clearly and uniformly defines when, how, and why companies can curtail free speech.

POLICY POSITIONS

United States

The practice among countries in the West has been to protect online freedoms. In the United States, the First Amendment to the U.S. Constitution guarantees the right to free speech, and numerous court rulings have set legal precedents in interpreting that provision. Guided by the long-standing position of the U.S. Supreme Court, U.S. policymakers have prioritized the protection of free speech over concerns about online privacy. In the United States, privacy rights do not always apply once personal information becomes publicly available. As soon as data have been made public, free speech trumps privacy concerns. As the birthplace of the Internet and the leader of the global digital revolution,

the United States is also one of the staunchest supporters globally of Internet freedoms, a principled position that is nonetheless influenced by economic factors.

Because many of the world's most popular virtual platforms and social media companies are based in the United States, the American government has a vested economic interest in keeping the Internet and its content as unregulated as possible, giving companies the flexibility and freedom to develop new ways of using the Internet and to expand services to reach a wider audience. The combination of U.S. companies' dominance on the Internet and their inclination to adopt U.S. notions of free speech leads these companies to operate under a liberal interpretation of the freedom of expression online. Often, the popularity of U.S.-based virtual platforms and social networking sites and, by extension, American liberal traditions can be perceived as potential threats in jurisdictions that prefer stricter limits on free speech and espouse greater regulation of online content.

European Union

As the other pillar of the Western liberal order, the EU has a different perspective on the inherent tension between free speech and online privacy. In Europe, policymakers and institutions have striven to reach a more balanced assessment of the interaction between these two principles, with almost equal weight attached to the right to privacy as to freedom of expression. Europe interprets its free speech laws through two judicial bodies, the ECJ and the European Court of Human Rights. While hailed as a watershed for the European approach to the balance between free speech and privacy, the ECJ's May 2014 ruling on a landmark case regarding online privacy and Google also marked the ideological differences between the EU and the United States.[42] The court stated that "certain people can ask search engines to remove specific results for queries that include their name, where the interests in those results appearing are outweighed by the person's privacy rights."[43] Dubbed as the right to be forgotten, the ruling allows EU citizens to request uniform resource locators (URLs) to be taken down from Google's EU search engines (see box 1).

Box 1: Google and the Right to Be Forgotten

According to Google's removal request website:

> When you make [a request for specific search results to be removed], we will balance the privacy rights of the individual with the public's interest to know and the right to distribute information. When evaluating your request, we will look at whether the results include outdated information about you, as well as whether there's a public interest in the information – for example, we may decline to remove certain information about financial scams, professional malpractice, criminal convictions, or public conduct of government officials.[1]

To oversee compliance with the European Court of Justice decision that allowed users to make such requests, Google set up an expert advisory group that had seven members when it was established: Eric Schmidt, Google's executive chair; David Drummond, Google's chief legal officer; Frank La Rue, former UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression; Peggy Valcke, director of the law school of the University of Leuven; José-Luis Piñar, former head of Spain's data protection authority; Jimmy Wales, co-founder of Wikipedia; and Luciano Floridi, information ethics philosopher at the Oxford Internet Institute. If a request is rejected, an EU citizen may file an appeal with his or her home country's data protection agency.

In the first four months following the May 2014 court ruling, Google received 100,000 requests and approved more than 50 percent of them.[2] Of requests made to Google UK and Google Ireland, the leading reasons for content removal were: fraud or scam incidents (31 percent), arrests for violent or serious crime (20 percent), and child pornography arrests (12 percent). Germany, the EU's most populous country with 80 million people, made the most requests in the EU with 40 percent of the total, followed by Spain with 14 percent, the UK with 13 percent, and Italy with 3 percent. France, the EU's second-most-populous country with 67 million people, made only about 2 percent of the total requests in the EU.[3]

1. "Search Removal Request Under Data Protection Law in Europe," Google, last accessed December 22, 2015, https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=en.
2. Mark Scott, "Discussing Online 'Right to Be Forgotten,' Google Takes European Privacy Tour to Spain," Bits (blog), *New York Times*, September 9, 2014, http://bits.blogs.nytimes.com/2014/09/09/discussing-online-right-to-be-forgotten-google-takes-european-privacy-tour-to-spain/?ref=technology.
3. Danny Sullivan, "How Google's New 'Right to Be Forgotten' Form Works: An Explainer," Search Engine Land, May 30, 2014, http://searchengineland.com/google-right-to-be-forgotten-form-192837.

U.S. and EU approaches have therefore been different in areas where free speech has tended to clash with the need to protect online privacy. The cultural split between Americans and Europeans highlights fundamental disagreements over notions of the related but separate rights to privacy, free speech, and information. Such disagreements often lead to confrontations between dominant U.S. Internet companies doing business in Europe and the European governments trying to regulate them. Essentially, the cultural split turns into a battle "between two views of freedom – the US belief that free speech trumps everything, and the European view that individuals should have some control over what the world knows about them," as Rory Cellan-Jones of the BBC put it.[44]

Russia

Despite the alignment of Russian television stations and newspapers with Kremlin policies, the Internet in Russia had been largely uncensored until the last few years. But the tide is turning. Roskomnadzor, Russia's Internet oversight agency, has been at the helm of efforts to curtail the freedom of expression by targeting opposition voices. As the *Washington Post*'s Michael Birnbaum explained, a blogger law passed in July 2014 requires "any person whose online presence draws more than 3,000 daily readers to register [with Roskomnadzor], disclose personal information and submit to the same regulations as mass media [including a requirement to publish names and contact details]. . . . The rules also hold them liable for any misinformation that they publish — along with any misinformation contained in comments posted on their Web sites, even if the bloggers did not write the comments."[45] Bloggers and activists fear that the new regulation "will encourage online self-censorship and will create new risks for those who advocate contrarian viewpoints," according to Birnbaum.[46] Roskomnadzor devotes about 35 people to its monitoring and registering effort and is automating some parts of the process.

A law that gives Russian authorities the power to block websites without any official explanation came into effect on February 1, 2014. One month later, four Russian opposition sites were blocked, including the blog of anticorruption politician Alexei Navalny, Russia's most prominent anti-Kremlin leader. Additional restrictions requiring Russian user data to be stored on Russian soil, thereby subjecting the data to Russian legal oversight and monitoring, went into operation on September 1, 2015.[47]

China

China has the largest online population, with 649 million users as of February 2015.[48] As foreign businesses and particularly social media companies eye the Chinese market for overseas expansion, the onslaught of information available online poses a threat to the country's tight censorship controls. Beijing has banned altogether websites like Google, Facebook, and Twitter, which provide online platforms for expression, organization, and community outside the reach of Communist Party officials. Chinese online services hire

so-called little secretaries to remove politically sensitive material,[49] and Internet trolls known as the 50 Cent Party receive money from the government each time they write a pro-government post or comment.[50] Although the Internet has been an essential and immensely profitable component of China's economic success, the open nature of global virtual platforms is viewed as a threat to the government's firm grip on political power.

Seeking to fill the void left by the prohibition of popular social media sites on the mainland, Chinese entrepreneurs have created dozens of online social platforms tailored to a Chinese audience. However, the boom of Chinese-specific social media and networking platforms such as the microblogging site Weibo is "at least partially attributable to the fact that it's harder for the government to censor social media than other information channels," according to U.S. management consultancy McKinsey & Company.[51] While Chinese netizens continue to seek other channels of expression on the Internet, their efforts are curtailed by the government's efficacy in blocking access to online content. Researchers at the Berkman Center for Internet and Society at Harvard University describe the sociopolitical function of Twitter as follows:

> The discourse in the politically engaged portions of Chinese Twitter suggests that Twitter serves an alternative public sphere. The political group is formed of journalists, lawyers, human rights activists, and scholars, who are free to discuss topics typically not permitted in China, such as the Tiananmen Square protests, Tibetan and Uyghur issues, political scandals, and pollution. Yet China's Internet repression is clearly succeeding. Chinese Twitter falls well short of supporting a broadly accessible networked public sphere. The proportion of the Chinese populace with direct access to the debates, communities, and shared resources on Twitter is relatively small, and the avenues by which such discourse might find its way into mainstream political discussion are severely constrained. The firewall between Twitter and the much larger social media platforms in China remains a formidable barrier.[52]

For years, Chinese officials have been tacitly turning a blind eye to netizens using virtual private networks (VPNs) to circumvent the Chinese firewall. Such access to online social platforms like Facebook and Twitter has created a new medium through which Chinese citizens can more freely express themselves despite severe restrictions imposed on them. But now the government has blocked VPN access and demanded that users register their real names, as opposed to virtual identities, on an array of Internet services. As Chinese netizens try to buck the online constraints placed on them, the Chinese government continues to clamp down on dissent and challenges to authority on the Internet.

Iran

Iran also exercises tight control over what is published on the Internet, but its policies have a religious tint, monitoring content for violations of sharia law. Like China, Iran blocks access to Facebook and Twitter, in addition to YouTube. Millions of tech-savvy us-

ers, however, easily get around the bans by using VPNs, and Iran's supreme leader, Ayatollah Ali Khamenei, even has his own Twitter page in multiple languages.[53]

Even though users bypass Iranian firewalls, they are still monitored by the Iranian government. Iranian state television reported in early 2015 that the Iranian government was monitoring 8 million Facebook accounts with new software under its Spider program. Established in 2007, the Center for Investigation of Organized Crime is the branch of the elite Iranian Revolutionary Guard Corps that monitors the Spider program, which targets and arrests Facebook users who spread immoral content.[54] The center claims that Facebook is "trying to push its users toward immoral content via its suggestion system, by making them choose harmful, decadent and obscene content over beneficial and educational subject matter," Reuters reported.[55] In the wake of evidence pointing to the potency of the Internet in destabilizing regimes, the Center for Investigation of Organized Crime will expand its Spider program to monitor other social media, including Instagram, Viber, and WhatsApp. Moreover, in December 2014, Iranian Communications Minister Mahmoud Vaezi introduced a policy of smart filtering to improve the efficacy of the government's censorship. In the summer of 2015, Vaezi reported that a second stage of the policy had been launched.[56]

POLICY INITIATIVES

There is already an overarching multilateral framework that protects the freedom of expression online. The UN's Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights constitute the main pillars of the international regime for the protection of online free speech. Frank La Rue, the former UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression, emphasized that "by explicitly providing that everyone has the right to express him or herself through any media, article 19 of the Universal Declaration of Human Rights and the Covenant was drafted with foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression. Hence, the framework of international human rights law remains relevant today and equally applicable to new communications technologies such as the Internet."[57]

So the issue is not so much the definition of multilateral rules for protecting online freedoms as it is the nature of the government practices that constrain these freedoms. In many ways, this is a discussion that harks back to traditional divisions regarding the scope of fundamental freedoms in liberal versus authoritarian regimes. In that sense, the online universe is a replica of the real world, where these freedoms are protected or violated, as the case may be. The real difference in terms of the protection of free speech online versus offline lies in the incommensurately bigger role that large Internet companies play almost as arbiters of these rules in the digital world. The emergence and growth of the Internet

has shifted the power of enforcement away from governments. Due to their function as enablers of global conversations, the Twitters and YouTubes of this world have—maybe unwittingly, but quite inevitably—been thrust into such a role and are striving to find the right approach to collaborate with governments inclined to expand the implementation of their national laws into the virtual space.

Governments can ask for specific content to be removed from these platforms if they claim that the content is in violation of their country's domestic laws. Google, Twitter, LinkedIn, Yahoo, and Facebook have started to publish transparency reports, which tally government requests for content removals.[58] For the first six months of 2015, Twitter received 1,003 such removal requests.[59] The figure for Google for the second half of 2014 was almost three times as high, at 3,523.[60]

Internet companies have so far used disparate methods for assessing and complying with these requests. For instance, Twitter reported that in only 42 percent of the requests made in the first half of 2015 was content removed.[61] But by being nontransparent, ambiguous, and inconsistent in their content regulation policies, social media companies risk haphazard implementation that harms the public and tarnishes their image. The details and criteria of the decisionmaking processes to remove content are not transparent, leading observers to question when, how, and to what extent companies can unilaterally delete online material.

The language of social media companies' community standards is often ambiguous and subjective. Popular online platforms such as YouTube, Facebook, and Twitter all provide user guidelines on hate speech stating that they do not tolerate content that promotes or condones violence based on discriminatory traits like race, ethnicity, religion, disability, nationality, age, and sexual orientation. However, none of these social media companies provides specific details about the methods or standards for deciding what does and does not warrant removal. The phrasing of these policies leave them open to interpretation, with each social media company unilaterally deciding to which cases its policy applies.

The language of social media companies' community standards is often ambiguous and subjective.

According to its community guidelines, YouTube and its products are "platforms for free expression," with the caveat that determining what content to remove "can be a delicate balancing act, but if the primary purpose is to attack a protected group, the content crosses the line."[62] No further information is given on where that line is drawn or what criteria are considered in the balancing act. Twitter warns that because of the diversity of "voices, ideas and perspectives" available on its network, users "may encounter content [they] con-

sider to be inflammatory or inappropriate that is not considered a violation of our rules."[63] In the case of Facebook, the social networking platform concedes that "sometimes people share content containing someone else's hate speech for the purpose of raising awareness or educating others about that hate speech" but says nothing about how the company determines where it draws the line between the positive and negative consequences of sharing hurtful or violent content.[64]

The Freedom Online Coalition was set up in 2011 at the initiative of the Netherlands, which convened the coalition's maiden meeting. As of late 2015, the group had assembled 29 states that aim to "work together to support Internet freedom and protect fundamental human rights – free expression, association, assembly, and privacy online – worldwide."[65] The group has adopted a set of recommendations to better protect online freedoms, ranging from calls on governments to end repressive measures such as censorship and harassment that undermine the freedom of expression online to improvements in the domestic oversight of surveillance practices.[66]

Another dimension of the collaboration between governments and global social media sites relates to the online effort to combat extremism. Governments as well as Internet and social media companies struggle in their attempts to curtail the growing online presence of violent extremist groups like the Islamic State. The Internet allows such terrorist movements to spread information quickly and cheaply to a wide audience, regardless of a user's location or device.

Social media companies have faced fierce criticism for allowing the Islamic State to use platforms like Twitter to meet these ends. A U.S. study commissioned by Google Ideas and published by the Brookings Institution in March 2015 estimated that there were at least 46,000 Twitter accounts linked to the Islamist group.[67] Twitter's violations department suspended approximately 10,000 accounts in one day on April 2, 2015, and the social network had earlier acknowledged that it had suspended as many as 2,000 Islamic State–related accounts per week in the previous months.[68] The arduous task of tracking down and suspending Islamic State–linked accounts is further complicated by the fact that suspended users are still able to create new accounts.[69]

In response to this formidable challenge, social media companies are being proactive in anticipating corrupted use of their online platforms. Facebook, Twitter, YouTube, and others have terms of use regarding images of gratuitous violence or content that incites hatred. These sites also terminate accounts that are registered to members of foreign terrorist organizations designated by the U.S. State Department and are used in an official capacity to further the interests of these organizations.

Almost as a harbinger of the type of collaborative efforts that may emerge, international law enforcement agencies have joined forces with social media companies to combat

foreign jihadists online. Since July 2015, Europol, the European police agency, has been working with unnamed social media companies to track down accounts associated with the Islamic State. Europol aims to close down new Islamic State–related accounts within two hours of their creation, but this goal is daunting given the large number of such accounts that are being set up every day.

TRANSATLANTIC ROAD MAP

Both the United States and the EU have set out Internet freedoms as a core objective of their cyberdiplomacy. The White House's International Strategy for Cyberspace stipulated that the "the United States will be a tireless advocate of fundamental freedoms of speech and association through cyberspace . . . and will work to encourage governments to address real cyberspace threats, rather than impose upon companies responsibilities of inappropriately limiting either freedom of expression or the free flow of information."[70] Similarly, the EU's cybersecurity strategy of 2013 and the EU Council Conclusions on Cyber Diplomacy of February 2015 have tasked EU institutions and member states to advance the cause of Internet freedoms.[71] The latter document called on the EU "to encourage exchanges of good practices on the promotion and protection of fundamental rights in cyberspace with all relevant stakeholders, in particular the freedom of opinion and expression and the right to privacy."[72] So far, Washington and Brussels have incorporated these objectives into their bilateral outreach efforts with third countries, in particular as part of their cyberpolicy-related dialogues.[73] More effective outcomes can be achieved in at least two areas with a more collaborative effort by the transatlantic partners.

Both the United States and the EU have set out Internet freedoms as a core objective of their cyberdiplomacy.

The first area is support for the Freedom Online Coalition. Despite an ambitious start, the growth of the coalition's membership base has been slow, possibly reflecting a deliberate decision by its founders to ensure that new members are in a position to meaningfully contribute to the agenda on issues related to online freedoms. The group needs a more diverse membership to be able to become a more influential agenda setter for online freedoms. Attracting new members to the coalition could become a shared objective of the transatlantic partners' cyberdiplomacy.

The second area is the elaboration of norms for the export of surveillance technologies. The EU and the United States have established a sound network of institutional collaboration on cyberpolicy themes through the Working Group on Cyber-security and Cybercrime, a group established in 2010 that focuses mostly on enhancing transatlantic collabo-

ration for managing cybersecurity incidents and combating cybercrime. There is also an annual EU-U.S. Information Society Dialogue on Internet policy and governance. Finally, the March 2014 EU-U.S. summit saw the launch of a new cyberdialogue for cross-cutting Internet governance issues, including foreign-policy-related matters. Given the need for illiberal regimes access to the latest technology to implement their campaigns to restrict Internet freedoms, this elaborate EU-U.S. institutional setup can and should be used to develop a code of conduct related to the export of products and technologies that could be used for surveillance or censorship by these regimes.

CHAPTER THREE

DATA FLOWS

A significant impact of the lack of global norms on data privacy can be seen in the restrictions that states impose on the safeguarding and transfer of data, with adverse consequences for global welfare.

The transition to a digital world has triggered substantial changes in the structure of the global economy. Empowered by greater availability of data, the development of global production chains has accelerated, leading to more trade and investment flows worldwide and raising income levels in both developed and developing economies. The McKinsey Global Institute estimated that between 2005 and 2010, the Internet contributed more than 10 percent of gross domestic product (GDP) growth in Canada, France, Germany, Italy, Japan, South Korea, Sweden, the UK, and the United States, and more than 20 percent of GDP growth in Brazil, China, India, and Russia.[74] The same institute published another report in 2014 stating that online traffic across national borders had grown eighteenfold between 2005 and 2012, and that the global flow of goods, services, and investments, which reached $26 trillion in 2012, could more than triple by 2025.[75]

The ubiquity of data has also given rise to new services. Taking advantage of big data, companies have overhauled their customer relations management, streamlined their production schedules, and started to explore new markets. The Internet has transformed the way in which many goods and services in the economy are produced and delivered. As

an OECD study found, "Digital sales make up more than half of music industry revenue; the share of digital sales for games, videos, and books are smaller, but growing quickly."[76] This world of abundant data has at the same time created new business models that rely on cloud computing, which in turn necessitates the centralization of data collected from many different corners of the globe.

Yet these models and services are now at risk as states seek to impose new rules constraining the storage and transfer of data. There are two general categories of barriers to the storage and transfer of information: data localization requirements and restrictions on the flow of data across national borders.

Data localization requirements relate to government measures that compel companies to store personal and commercial information in data centers that are physically located on their territories. These rules generally aim to protect the online privacy of citizens against the intrusion and surveillance of foreign powers. In other cases, these requirements stem from a flawed expectation that regulatory monitoring of some industries—like financial services—can be better managed if the required data are stored in a country's own servers.

Data-driven models and services are now at risk as states seek to impose new rules constraining the storage and transfer of data.

Data localization also raises fears about the fragmentation of the Internet. According to current practice, companies can use one jurisdiction in which their data servers are based to centralize their data and develop their associated services for a global audience. But as more and more states start to impose similar requirements, companies will be unable to aggregate data in one location and will be forced to host separate data servers. Companies will then need to be selective in their investment decisions related to the location of their data servers and forego such investments in countries where domestic markets cannot, on their own, economically justify this decision. As a result, services will become unavailable in these markets. That will substantially reduce the geographic scope of the services offered, with a detrimental impact not only on companies' balance sheets but also on the denizens of all excluded countries.

Opponents of data localization rules also argue that they tend to weaken data security. The multiplication of these rules will lead to a proliferation of data centers within various jurisdictions with significantly different data storage and protection standards and technologies. The outcome will be a multitude of data pools that can be more easily targeted by hacker groups, as opposed to better-protected globalized data hubs.

Cross-border data flows can also be impeded as a result of domestic regulation that sets conditions for the international transfer of personal or commercial data. Amid a growing

recognition of the importance of data privacy and confidentiality challenges, states have overhauled their domestic legislation to address these concerns. But an unintended consequence of these amendments has been the creation of an environment that makes it more difficult to share personal and commercial data around the world.

POLICY POSITIONS

United States

Unlike the EU, the United States has no unified regulatory framework on data privacy at the federal level. Data privacy is regulated as a patchwork of federal and state legislation. There are about 20 sector-specific national privacy and data security laws in addition to hundreds of such laws in the country's 50 states. Sector-specific restrictions have been set out for some sensitive issues such as health records, credit reports, financial information, communications, and student records.[77] The U.S. Federal Trade Commission is the government agency entrusted with enforcing a privacy framework on data handlers.

The lack of a federal-level regime has led to complaints about the inadequacy of the protection of consumer privacy. As a result, in February 2015, Obama proposed a new Consumer Privacy Bill of Rights, a draft law intended to govern the collection and distribution of consumer data by requiring industries to develop their own codes of conduct for ensuring data confidentiality. Companies will also be required to set up privacy review boards to be overseen by the Federal Trade Commission.

In addition, the United States has no geographic transfer restrictions for data—the one exception being with regard to accountants who transfer tax preparation materials.

European Union

The master legislation for data privacy and data transfer rules in the EU is the Data Protection Directive of 1995.[78] The EU is set to adopt new data protection legislation in early 2016 in the wake of the agreement reached in December 2015 between the European Parliament and the European Council on the main provisions of this important package. The EU has developed a framework based on this legislation that allows the transfer of data to states that are considered to have adequate data privacy safeguards. Accordingly, the EU allows the personal data of EU citizens to be transferred only to third countries deemed to grant equally strong protection of personal data. As of early 2016, this list is limited to Andorra, Argentina, Canada, the Faeroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay. Due to differences in regulatory approaches, the United States is not on the list.

To allow the transfer of data to U.S.-based entities, the European Commission and the U.S. Department of Commerce negotiated a set of principles known as the Safe Harbor

arrangement to mirror the commitments under the EU directive. By voluntarily joining the arrangement, U.S. companies agreed to adopt stringent data protection regimes that provided a similar level of oversight of data confidentiality to that guaranteed in the EU. As of October 2015, a total of more than 4,500 U.S. companies were using this framework.[79] Firms that opted in to this program were presumed to offer an "adequate level of protection" and could therefore become recipients of private data transfers from EU countries. In reality, the Safe Harbor arrangement bound U.S. companies to EU data protection rules. Furthermore, non-U.S. and U.S. firms alike were allowed to use EU-approved model contracts containing clauses based on EU standards known as binding corporate rules for data transfers between subsidiaries.

With the Snowden allegations, however, it became clear that the modalities of the agreement had been gravely violated, as many large Internet companies that had adopted Safe Harbor principles were also involved in the U.S. government's PRISM surveillance program that Snowden uncovered. The EU charged the United States with breaching trust in the Internet and threatened to end the Safe Harbor arrangement. The European Commission believed that Safe Harbor acted as "a conduit for the transfer of the personal data of EU citizens from the EU to the US by companies required to surrender data to US intelligence agencies."[80]

An additional layer of complexity was added to this debate in October 2015, when the ECJ ruled the Safe Harbor agreement to be inadequate in protecting the confidentiality of EU citizens' private data in the face of the aggressiveness of the U.S. government's online surveillance and data capture practices. The ECJ ruling ended the application of Safe Harbor, bringing a degree of uncertainty to the legality of the cross-border data transfer practices of many companies, large and small.[81] The decision will force Brussels and Washington to negotiate a new agreement, Safe Harbor 2.0, which will require non-European companies to comply with the stricter provisions regarding data confidentiality that the ECJ set out.

China

Chinese legislation contains many provisions that create severe obstacles to the transfer of data abroad. For instance, standards adopted by the Standardization Administration and the General Administration of Quality Supervision, Inspection, and Quarantine—two government bodies—prohibit overseas transfers of data without express user consent or government permission. A report by the European Center for International Political Economy that analyzed the relevant Chinese legislation found that despite the voluntary character of these guidelines, they serve as a "regulatory baseline" for law enforcement and are de facto data localization laws for all business sectors.[82] In financial services, the legislation incorporates a strong data localization requirement as service providers are prohibited

from storing, processing, or analyzing offshore any personal financial data belonging to Chinese citizens.

Russia

In September 2015, Russia changed its privacy legislation to include a clear data localization requirement. The new law obliges data operators to ensure that any collection or use of personal data of Russian citizens is carried out with databases located inside Russia. A policy brief by the European Center for International Political Economy estimated that the losses from this amendment represented 0.27 percent of Russia's GDP in 2015, equivalent to $5.7 billion.[83]

India

Indian legislation allows sensitive personal data to be transferred abroad only when necessary or when the individual's consent has been obtained. But an exception has been carved out for India's burgeoning outsourcing business. Indian Prime Minister Narendra Modi's government has also banned the use of private e-mail servers like Gmail and Yahoo for official government use.[84]

POLICY INITIATIVES

At present, there are no binding multilateral rules that regulate cross-border data flows. For Western economies, the OECD has developed a set of draft guidelines to better balance the requirements of liberalizing cross-border data flows with calls to address privacy concerns.[85] The guidelines highlight the need for improved interoperability for enhanced data protection at a global level and recommend that rules restricting data transfer be proportionate to the associated privacy risks.

An important regional initiative was undertaken in 2004 by the Asia-Pacific Economic Cooperation forum (APEC), which developed a privacy framework designed to guide the preparation of national privacy laws among APEC members. The framework seeks to strike a balance between the enforcement of privacy rules and the need to maintain an open environment for cross-border data flows.[86] The framework would prioritize the ability of a data recipient to protect the information received over the more specific requirements of national legislation on data privacy and confidentiality. In other words, even if national laws are deemed to be inadequate in ensuring a standard of data protection equivalent to that of the originating country, cross-border data transfers will still be allowed because of the stronger protection guaranteed by

At present, there are no binding multilateral rules that regulate cross-border data flows.

the corporate practices of the receiving entity. Building on its existing approach to cross-border data transfers, in 2012 APEC promulgated a set of Cross-Border Privacy Rules designed to safeguard personal data throughout the Asia-Pacific region.

The 2010 free trade agreement between the United States and South Korea is the first bilateral preferential trade deal to incorporate specific provisions on cross-border data flows. The agreement states that "recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[87] The nonbinding language weakens the commitment to liberalize data flows but indicates a shared awareness of the importance of this objective and a political willingness to find the right balance between privacy and the free flow of cross-border data.

The recently concluded Trans-Pacific Partnership (TPP), a new-generation free trade agreement between the United States and eleven other mostly Asian countries, incorporates provisions designed to lift obstacles to cross-border data flows. The accord requires participating countries to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person." But this requirement is not absolute because contracting states can still impose restrictions on cross-border data transfers to "achieve a legitimate public policy objective."[88]

The topic of cross-border data flows has also been part of the agenda of the Group of Twenty major economies (G20) and its associated body, the B20, which assembles business leaders from the G20 nations. As a part of its recommendations to improve the global trading system for the emerging digital economy, the B20 working group on international trade called for a rollback of data flow restrictions and an improvement of standards for cross-border data security. The B20 working group advised G20 governments in particular to adopt the accountability principle to eliminate barriers to cross-border data flows. The group's recommendations stated that "the accountability principle places responsibility on the organisation carrying out the cross-border transfer, rather than on the data subject or regulatory authority. The transferring organization has an affirmative responsibility to establish rules and procedures that achieve actual data protection, or to participate in a system that does so."[89] Typical examples of such systems include the U.S.-EU Safe Harbor agreement and the APEC Cross-Border Privacy Rules.

TRANSATLANTIC ROAD MAP

Given that there is no multilateral regime on cross-border data flows, this policy domain offers an opportunity for the transatlantic partners to demonstrate collective leadership. A

joint U.S.-EU approach, especially in view of the weight of these two blocs in the digital economy, can easily become a global standard.

The negotiations on the proposed Transatlantic Trade and Investment Partnership (TTIP) offer a sound platform for the two sides to discuss this topic. But despite a U.S. desire to do so, the EU has resisted including data privacy and data migration issues in the scope of TTIP, arguing that the EU should first legislate internally before it can genuinely negotiate with the United States. The European Commission has stated that data protection standards will not be negotiated in TTIP.[90] But this categorical position hinders a much-needed standard-setting effort in the area of data policy. It also contravenes the whole spirit of TTIP, which has been branded as a forward-looking trade treaty to establish global norms on trade and investment. Indeed, TTIP's credibility as the benchmark for other twenty-first-century trade agreements would be imperiled if the deal reached were to totally circumvent such a core component of the digital economy. A joint U.S.-EU approach to cross-border data flows codified under TTIP could serve as a blueprint for the ongoing negotiations on the Trade in Services Agreement (TiSA), a proposed international trade deal that is set to affect the services sector, which produces 70 percent of global GDP.[91]

An option to foster a joint approach is for the EU to adopt its renewed data privacy legislation before the conclusion of the TTIP negotiations, so that issues of data privacy and cross-border data flows can be properly addressed under TTIP. The expected adoption in early 2016 of the General Data Protection Regulation should encourage the EU to be more lenient about conditions for data transfer in TTIP. Meanwhile, the two transatlantic partners should seek to reach an agreement on a new Safe Harbor arrangement. In its post-Snowden analysis of Safe Harbor, the European Commission called on the U.S. Federal Trade Commission to improve the enforcement of the principles applicable to adhering companies and their subcontractors.[92] The commission asked that these principles be incorporated more effectively into firms' privacy policies and be made available to the public. In its opinion, the European Data Protection Supervisor further suggested "[increasing] the degree of liability of European data controllers for checking that companies located in the US which claim to comply with the Safe Harbour principles effectively do so."[93] A key consideration in the conclusion of a renewed Safe Harbor arrangement will be whether the United States will adopt legislation to grant judicial redress to EU citizens for alleged breaches of data confidentiality.

But these options still rely on the assumption that data flows cannot be fully liberalized unless the EU's trading partners adhere to its norms on data confidentiality. The question is whether, despite the current political momentum in favor of far-reaching privacy legislation, Brussels can be persuaded to adopt a more flexible stance on data flows. In other words, will the EU revisit its position of wanting to impose its own privacy regulations on all its trading partners as a condition of data transfers?

To eliminate the detrimental impact of regulatory differences on trade, the transatlantic partners have through TTIP developed an approach defined as mutual equivalence, which amounts to the recognition by the United States and the EU of each other's regulatory regimes. For data policy, this would entail the development of a common code that stipulates the minimum regulatory requirements that third countries have to fulfill to be qualified as safe destinations for data transfers. In an early reaction to the EU's draft regulation on data privacy, the United States asked for a "greater opportunity to recognize codes of conduct developed by the multistakeholder process advocated in the blueprint and also in OECD recommendations to which EU member states are parties."[94] Some of the principles codified in the APEC privacy framework could be borrowed in this respect. Also, as the German government suggested, the partners could seek to establish a distinction between personal and commercial data and codify more flexible norms for the cross-border transfer of commercial data.[95]

The transatlantic partners could jointly or separately aim to develop interoperable mechanisms among different privacy regimes.

In the same vein, the transatlantic partners could jointly or separately aim to develop interoperable mechanisms among different privacy regimes. In the context of negotiating the draft EU Regulation on Data Privacy, the European Parliament proposed the concept of a European data protection seal, which would allow certified organizations to transfer personal data to one another. To begin to align the compliance requirements of the EU's binding corporate rules, APEC's Cross-Border Privacy Rules, and the proposed European data protection seals would represent one of the most effective strategies for delivering consistent privacy protections globally while allowing for more coherent data transfer regimes.[96]

CHAPTER FOUR

INTERNET GOVERNANCE

There are few issues more appropriate than the debate on governing the Internet to illustrate the variety of perspectives on the future of global cybergovernance. At the core of the debate is the scope of governments' roles in shaping the global rules for the Internet. At one end of the spectrum lies a group of countries led by Russia and China that are proponents of a multilateral governance model that gives exclusive competence to governments for managing the Internet. This intergovernmental approach stands in stark contrast to the current setup, which reflects the preference of the more liberal members of the international community for a multistakeholder model in which governments, industry representatives, user groups, and academic entities also have a role in the governance structure.

Currently, the Internet Corporation for Assigned Names and Numbers (ICANN) provides the multistakeholder Internet governance model, after the U.S. government's National Telecommunications and Information Administration granted ICANN a key management contract in 1999.[97] This contract involves managing the database that connects domain names, such as .com, .org, and .co.uk, to their numeric IP addresses—which adds up to a significant amount of control of today's Internet. Most of the central root servers that manage these assignments are located in the United States. Companies outside the United States were not allowed to compete for this contract, and the fact that this central component is controlled by the U.S. government—with changes to top-level domains passing through the U.S. Department of Commerce—has long been a point of conten-

tion, opening the United States to accusations of Internet imperialism. Claims of Western mercantilism have been given additional credence by ICANN's four-year delay—allegedly caused by EU and U.S. governments intent on safeguarding the commercial interests of their companies—in rolling out new top-level domain names for users who speak languages with non-Roman scripts like Chinese, Arabic, Persian, and Russian.

Beyond ICANN's symbiotic relationship with the U.S. government, the corporation's structure as a multistakeholder body has also been challenged by a range of global and emerging powers. These powers aspire to increase the influence of governments relative to other stakeholders such as academic institutions, user groups, or technical bodies that are parts of the governance structure. The current debate therefore pits a group composed primarily of liberal democracies including EU countries and the United States, which defend the multistakeholder model, against a group of cybersovereignty advocates, including China and Russia, that wish to either retain or claw back governmental control of cyberspace.[98] Swing states like India and Brazil fall between the two camps.[99]

POLICY POSITIONS

United States

For the United States, the multistakeholder governance model works. Only this model has the flexibility and adaptability to ensure that the extraordinary growth of the Internet will continue along with the economic prosperity it has helped create.[100] In a way, despite the de facto U.S. dominance of the DNS (Domain Name System), the Internet has flourished due to the hands-off approach encapsulated in the current ICANN multistakeholder model.

European Union

The EU supports the continuation of multistakeholder governance. It has adopted an ICANN-like model for the governance of the .eu domain name with the establishment of the European Registry for Internet Domains as a private, transnational, not-for-profit company.[101]

At the same time, Brussels challenges U.S. stewardship and the U.S.-centric model of Internet governance.[102] In a 2014 statement, the European Commission called for more "transparent, accountable and inclusive" Internet governance, referring specifically to the "large-scale internet surveillance" by the United States and the resulting "reduced trust in the internet."[103]

China

China's position is that an intergovernmental approach should replace the current multistakeholder model of governance. This position is fully compatible with Beijing's view that only the Chinese government can be the legitimate representative of the Chinese people on the international stage.

As a result, Beijing wants the UN and its agencies that involve only government representatives to have a role in the management of the Internet. The Chinese government's white paper on this topic stated that "China holds that the role of the UN should be given full scope in international Internet administration. China supports the establishment of an authoritative and just international Internet administration organization under the UN system through democratic procedures on a worldwide scale."[104]

Russia

Russia is also pushing for a more state-centric system to manage the Internet. Just as is the case with China, Russia's proclivity for favoring intergovernmental regulation is shaped by a desire to construe the Internet as a vehicle for legitimizing national measures to control citizens. Russia views the current system as designed to serve the commercial and geopolitical interests of the United States and other Western countries and to sustain their dominance of the Internet.[105]

The convergence between Moscow's and Beijing's views on the governance of the Internet was reflected in a bilateral treaty signed by Russia and China in May 2015 on cooperation in the field of international information security. The treaty calls for the creation of a multilateral, democratic, and transparent management system for the Internet, championing a predominant role for governments in Internet governance.

India and Brazil

Among the constellation of emerging powers, Brazil and India represent two different approaches.

New Delhi has championed the intergovernmental and multilateral option. India's argument is that only governments, by working through international organizations like the UN, have the legitimacy to make decisions on such important transnational issues.[106]

India also maintains that the multistakeholder model works against the interests of developing countries because they have fewer societal resources to participate in and shape the agenda of such a forum. Accordingly, in 2011 India introduced a proposal in the UN General Assembly to constitute a UN Committee for Internet-Related Policies, a multilateral governmental body that would have consisted of 50 UN member states chosen on the basis of equitable geographical representation. The Indian proposal would have elevated the role of governments in decisionmaking while constraining other stakeholders to mere advisory roles. However, the Modi government in office since May 2014 seems inclined to shift India's position toward a multistakeholder approach. At the June 2015 ICANN meeting, Indian Minister of Communications and Information Technology Ravi Shankar Prasad announced India's support for the multistakeholder model of Internet governance.[107]

Brazil had initially argued for multilateral governance of the Internet. In a speech to the UN General Assembly in 2013, Brazilian President Dilma Rousseff called for more intergovernmental influence over the global management of the Internet. But after recognizing that the Snowden incident had created an opening for her to redefine Brazil not only as a proud supporter of the multistakeholder approach but also as a more reliable champion of global Internet governance than the United States, she later revised her position.[108] This change helped Brasília overcome the discrepancy between its domestic structure of Internet governance, which reflects a genuinely multistakeholder model, and the country's international position.

POLICY INITIATIVES

The reform of Internet governance has been on the agenda of several international efforts. The World Summit on the Information Society was created by a UN General Assembly resolution in December 2001. The initiative took the form of two conferences: the Geneva summit in December 2003 and the Tunis summit in November 2005. With the participation of heads of state and government and ministers from 175 countries as well as high-level representatives from international organizations, the private sector, and civil society, the Geneva summit ended with the Geneva Declaration of Principles and Geneva Plan of Action, with a call to establish the foundations of an inclusive information society. The objectives of the Tunis summit were to put the Geneva Plan of Action into effect and to reach agreements in the fields of Internet governance and financing mechanisms for a more equitable development of the Internet.[109] The Tunis meeting also framed the current definition of Internet governance as "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[110]

The World Summit on the Information Society also established the Internet Governance Forum, an ongoing policy dialogue that has met regularly since 2006 to discuss global issues of Internet access and use. The forum makes no recommendations and does not set standards but rather brings together thousands of people to discuss, debate, and network with other stakeholders who work on Internet governance issues.[111] Although some critics say that the Internet Governance Forum has no real influence, others argue that its lack of official authority provides a less formal environment to discuss controversial Internet issues and network with other stakeholders in the Internet governance debate.[112]

As a follow-up to the World Summit on the Information Society, a World Summit on the Information Society Forum was co-organized by the International Telecommunication Union (ITU); the UN Education, Scientific, and Cultural Organization (UNESCO); the UN Development Program; and the UN Conference on Trade and Development. The

forum, held in 2015, was the world's largest gathering of information and communications technology (ICT) stakeholders in the development community. The forum aimed to create a multistakeholder platform for exchanging information, creating knowledge, and sharing best practices linking the ICT universe with the global development agenda.

In April 2014, Brazil hosted NETmundial, a global multistakeholder meeting at which discussions were held on a road map for Internet governance. The meeting was designed to demonstrate the feasibility of the multistakeholder approach to Internet governance. Russia and India refused to back the concluding statement in favor of multistakeholder principles. Nonetheless, to support this meeting, the World Economic Forum launched the NETmundial Initiative in partnership with ICANN.

More divisive debates took place under the aegis of the ITU, the UN organization responsible for the global management of telecommunications and related technologies. At the 2012 Dubai meeting of the World Conference of International Telecommunications, an ITU forum in which countries met to discuss how to further economic and social development through efficient telecommunications services, China, Iran, Russia, Saudi Arabia, and others introduced proposals to extend the jurisdiction of the International Telecommunication Regulations, a binding ITU treaty, to the Internet. These proposals, which aimed to bring the Internet largely within the fold of the ITU,[113] were resisted by 55 states, including the United States and France.[114] The United States, the EU, and their allies contended that the Internet should remain outside the regulation of the ITU and that it did not belong in the International Telecommunication Regulations. Supporting the extension of the regulations were OECD members Mexico, South Korea, and Turkey. In the event, after two weeks of complex negotiations and despite the backing of 89 countries, the proposals failed.[115]

In April 2014, Brazil hosted NETmundial, a meeting designed to demonstrate the feasibility of the multistakeholder approach to Internet governance.

The United States saw the failure of the proposals as a victory, claiming that the Internet had never needed UN regulation and that the ITU treaty was, in the words of the head of the U.S. delegation, "inconsistent with the multistakeholder model of internet governance."[116] In discussing the ITU treaty, a bipartisan group of U.S. lawmakers described the attempts to extend the document's telecommunications remit to the Internet as a "power grab."[117] Countries that unsuccessfully supported the extension of the International Telecommunication Regulations claimed the opposite—that the treaty enabled standardization as it had done historically with dialing codes and phone keyboards. They argued that lobbying against the treaty was more about protecting a Western-dominated, U.S.-centric Internet administration.

These divisions emerged again at the fifth meeting of the ITU's World Telecommunication/ICT Policy Forum in May 2013 and at the UN in 2014, when a resolution was introduced in the General Assembly on reviewing the implementation of the outcomes of the World Summit on the Information Society. The resolution defined the review as an intergovernmental negotiation process, in defiance of the multistakeholder approach of the summit itself.

TRANSATLANTIC ROAD MAP

The topic of Internet governance is the area of cyberpolicy in which the U.S. and EU viewpoints are most closely aligned. Both partners value an open, free, and global Internet and believe that the current multistakeholder model should be preserved. They also seem willing to carry out reforms to enhance the inclusiveness and transparency of the U.S.-centric model of Internet governance. As a response to criticism of the U.S.-centric management of the Internet, the U.S. government announced in March 2014 that it would give up its control of ICANN and deepened its dialogue with the EU over the future of Internet governance. The topic was included for the first time on the agenda of the U.S.-EU summit that took place in the same month.

The transition of the Internet Assigned Numbers Authority (IANA), a department of ICANN, from U.S. control to a global stakeholder group was scheduled for the end of 2015 as a symbolic step to demonstrate that the United States was willing to respond to grievances about its hegemony over the management of the Internet.[118] As of November 2015, the group had finalized all but one item in its transition proposal. To underline the importance of this transition, ICANN Chief Executive Officer Fadi Chehadé stated publicly that "it has always been envisaged, including [by being] written into the founding agreements, that the special relationship between ICANN and [the] US government will become more global in the future, and less focused on one government. . . . The solution is not to replace one government with another."[119]

The United States and the EU should seek to empower ICANN's Government Advisory Committee to address the criticisms of states desiring more state-centric decisionmaking. The committee provides advice on public policy issues and the governance of ICANN. A reinforced committee could enhance the role of governments and their influence on ICANN's overall decisionmaking without sacrificing the organization's inherent pluralism.

As suggested by a Council on Foreign Relations report, the transatlantic allies should also contemplate strengthening the Internet Governance Forum financially and structurally, possibly by increasing the frequency of its meetings.[120] The forum's secretariat could be allocated specific funds to incentivize and subsidize the attendance of participants from the developing world as a formula to improve the body's inclusiveness.

Although developing countries are open to the participation of various stakeholders in Internet governance bodies in theory, these countries have difficulty in ensuring an adequate level of involvement in practice. This discrepancy is due to the challenge of finding the right people with sufficient technical expertise, English-language skills, and funding to participate in these forums, leading to an underrepresentation of Internet users from the non-English-speaking and developing worlds in organizations like ICANN.[121]

The United States should welcome the EU's efforts to act as an honest broker to win additional support from the developing world for multistakeholder governance of the Internet.

Finally, the United States should welcome the EU's efforts to act as an honest broker to win additional support from the developing world for multistakeholder governance of the Internet. The EU has included the topic of Internet governance in its strategic dialogues with a number of partners. The European Commission has proposed setting up a Global Internet Policy Observatory in cooperation with Brazil, with a view to promoting more open and transparent Internet governance. This call is echoed by former Swedish foreign minister Carl Bildt, who as the chair of the Global Commission on Internet Governance has urged Europe to take a more active role in setting the standards that will govern international cyberpolicy.[122]

CHAPTER FIVE

ELECTRONIC COMMERCE

The Internet has revolutionized the way people buy and sell goods and services. The rise of electronic commerce, or e-commerce, has allowed sellers in one part of the world to instantly connect to customers thousands of miles away with a single click. E-commerce has been defined by the U.S. Department of the Treasury as "the ability to perform transactions involving the exchange of goods or services between two or more parties using electronic tools and techniques."[123]

The dramatic growth of the digital economy has fueled the birth of countless companies that rely on the Internet to provide their goods and services, introducing a host of new challenges for regulatory bodies. The e-commerce industry was worth more than $13 trillion globally in 2012 and accounted for nearly one-fifth of companies' turnover in some European countries.[124]

One of the major issues to be tackled in Internet commerce is how to tax goods and services that are bought and sold in virtual marketplaces. The fluidity of the online economy has led many businesses with a physical presence in one or multiple countries to create an online portal through which their customers can access what they are selling. The combination of online and offline presences of merchants complicates the application of traditional rules of taxation that rely on determining the size and location of commercial income and profits. The growth of international trade in digital products like downloadable music and movies adds another layer of complexity to questions about online taxation.

Additionally, there is widespread concern that without better tax regulation, multinational Internet companies will continue to exploit the disparate tax systems of different countries, sometimes engaging in tax avoidance tactics to minimize taxes on profits, with adverse consequences for governments' fiscal revenues. Governments want to constrain the abilities of multinational enterprises that use gaps in the interaction of different tax systems to artificially reduce taxable income or shift profits to low-tax jurisdictions. One of the more common tax avoidance practices is the so-called double Irish arrangement, which exploits differences between the U.S. and Irish tax codes to move profits from Ireland to zero-tax countries such as Bermuda.[125] Multinational companies exploit U.S. tax rules, which define residency based on the territory where a company is incorporated, and Irish tax laws, which define residency based on the place where a company is managed and controlled, to avoid paying billions of dollars in tax. To circumvent the highest U.S. corporate tax rate of 35 percent, Internet companies prefer to keep their profits abroad. According to a *Bloomberg Business* analysis of 304 corporations' securities filings, "Eight of the biggest U.S. technology companies added a combined $69 billion to their stockpiled offshore profits over the past year."[126] Companies want the U.S. Congress to approve repatriation tax holidays, which would allow firms to bring overseas funds back to the United States at lower rates, such as 5 percent. But critics say that arrangement would benefit only corporations and would do nothing to stimulate the economy.

Without a common working framework to systematically organize the digital economy, electronic commerce will continue to grow as policymakers' understanding of how to regulate it continues to wane.

POLICY POSITIONS

United States

Many of the companies that made it on to *Forbes*'s list of the world's most valuable brands in 2015 were U.S. technology giants that are household names all over the world (see table 1). Because a great number of the most profitable Internet companies are American, the United States has fought to keep taxation on Internet companies everywhere to a minimum, ensuring that U.S. firms continue to enjoy the benefits of a hands-off taxation approach. Many high-tech companies do not wish to see stricter rules regulating the digital industry, especially tax codes that would apply to companies that have a virtual but not a physical presence in a country.[127]

Table 1: **Selected Companies From *Forbes's* List of the World's Most Valuable Brands**

Company	Established	Brand Value (Billions)	Market Capitalization (as of May 2015, Billions)	Sales (Billions)
1. Apple	1976	$145.3	$741.8	$199.38
2. Microsoft	1975	$69.3	$340.8	$93.27
3. Google Inc.	1998	$65.6	$367.6	$65.98
5. IBM	1911	$49.8	$160.2	$93.36
7. Samsung	1969	$37.9	$199.4	$195.89
10. Facebook	2004	$36.5	$231.6	$12.47
13. Amazon	1994	$28.1	$175.1	$88.99
15. Cisco	1984	$27.6	$139	$48.08
17. Oracle	1977	$26.8	$187.6	$38.84
19. Intel	1968	$25.8	$147.2	$55.87

Source: Kurt Badenhausen, "Apple and Microsoft Head the World's Most Valuable Brands," *Forbes*, May 13, 2015, http://www.forbes.com/sites/kurtbadenhausen/2015/05/13/apple-and-microsoft-head-the-worlds-most-valuable-brands-2015/.

European Union

Unlike the United States, European countries have repeatedly proposed increased regulation of the digital economy and stricter taxation laws. Even though European countries are highly industrialized with a very skilled technical workforce, European Internet companies have largely failed to produce major players that can compete with the big U.S. names. As a result, European governments have attempted to at least make a profit from American companies operating in their countries.

France, Germany, and the UK have pushed to change tax rules that allow U.S. web giants to avoid paying much corporate tax in Europe. France has tended to be one of the main proponents of stricter tax regulations for digital companies. In 2013, the country called on the European Commission to draw up proposals to establish "a tax regime for digital companies that ensure that the profits they make on the European market are subject to taxation and that the revenues are shared between the Member States, linking the tax base to the place where the profits are made," as reported by the *Wall Street Journal*.[128] Although the French proposal did not get much backing at the EU level, Paris was able to pressure the online retailer Amazon to establish a local office in France so that sales to France-based customers would be taxable in that country.

Until that point, Amazon had been accounting its sales to all EU markets from its fiscal residence in Luxembourg. This scheme allowed Amazon to pay taxes only in Luxembourg. This so-called tax-shopping practice, whereby companies declare permanent establishment in a low-tax constituency like Ireland or Luxembourg, remains legal under EU rules, but it is the subject of increased criticism from governments eager to raise tax revenues. The concept of permanent establishment for tax purposes is denounced as anachronistic in an age when taxable revenues can be generated without a physical presence. Therefore, there is political pressure to amend the concept of permanent establishment to allow governments to better tax the virtual transactions of their citizens.

Developing Countries

Concerns about tax avoidance and the erosion of sovereign tax revenues are not specific to industrialized countries. In a UN-sponsored Financing for Development meeting in Addis Ababa in July 2015, developing countries called for a revision of the current international tax regime that is shifting tax rights from countries in the Global South to the Global North.[129] A 2015 study by the UN Conference on Trade and Development estimated that developing countries lose around $100 billion per year in revenues due to tax avoidance by multinational enterprises.[130] The study suggested replacing the present UN expert committee on taxation with a full-fledged agency with responsibility for shaping global tax rules.

POLICY INITIATIVES

The OECD has set out to overhaul the existing tax system to accommodate the pressing needs of regulating the taxation of the digital economy. Many OECD countries want to increase the regulation of e-commerce but face difficult questions as to how to go about placing restrictions and taxes on an intangible marketplace that is enmeshed in countries' social, political, and economic structures. In response to the prevalence of Internet companies' tax avoidance practices, the OECD published an Action Plan on Base Erosion and Profit Shifting (BEPS) in July 2013, at the request of the G20.[131] The action plan examined ways to amend the rules on permanent establishment to allow the taxation of Internet companies, even if they had no physical presence in a jurisdiction where they nonetheless sold products and services. The action plan is to be officially implemented following the political commitment given to the document by the G20 leaders at their November 2015 summit in Turkey.

TRANSATLANTIC ROAD MAP

Although it covers business models that go beyond the digital universe, an agreement on the main recommendation of the OECD-led Action Plan on Base Erosion and Profit Shifting would create a more predictable environment for the taxation of e-commerce.

Profit shifting by large Internet-based multinationals has become a policy issue that unites the developed and the developing worlds. Such an environment creates pressure for national governments to find ways to identify and tax the territorial aspects of the Internet-enabled operations of global companies. Failure to establish a common multilateral framework can easily lead to a proliferation of individual and disparate measures by sovereign states, with a detrimental impact on the global availability of Internet-supplied products and services.

Profit shifting by large Internet-based multinationals has become a policy issue that unites the developed and the developing worlds.

In that sense, the EU and the United States, as the world's largest economies and as OECD members, have a large responsibility for shaping the new rules that are set to emerge from the BEPS action plan. In the wake of the G20's full endorsement of the plan, which could allay problems of how to tax e-commerce, Brussels and Washington could provide joint leadership to generate more liberal commitments from the World Trade Organization (WTO) contracting states that are parties in the Trade in Services Agreement negotiations on e-commerce and related services.[132] More specifically, the transatlantic partners should seek the support of other TiSA negotiating states for a permanent and binding moratorium on customs duties on electronic communications. Furthermore, having backed demands for a more development-friendly digital trade taxation regime by endorsing the BEPS action plan, the transatlantic partners could seek to leverage this goodwill by securing more liberal commitments under TiSA in e-commerce-related policy areas in which there is already a common approach. In particular, this would include global practices that condition the supply of services to local establishment and data localization requirements.

CHAPTER SIX

CYBERSECURITY

Although the Internet has changed the world for the better in many ways, it has also made people more vulnerable than ever. The incidence of cyberattacks has risen in tandem with the expansion of the Internet. Cyberattackers steal the money, research, and sometimes even the identities of their victims. Whether they are motivated by financial gain or by political objectives, cyberattacks threaten the economic prosperity of companies as well as the critical national infrastructure that supports the basis of everyday life. According to a report by the software security firm McAfee, estimates of the cost of cyberattacks vary but can be as high as $400 billion each year.[133] Findings by the Center for Strategic and International Studies put businesses' annual global losses at between $300 billion and $1 trillion.[134]

Cyberattacks are cheap but effective, anonymous yet tailored to specific requirements. For example, in February 2015, the Dutch government's main websites were overloaded with incoming traffic in a distributed denial-of-service attack that sought to make web pages unavailable to users, causing the websites to shut down. Backup plans proved ineffective, and the vulnerability of the government's critical infrastructure was publicly exposed. Defense against such attacks takes time and money, but the software for such an attack can be bought illegally for as little as $25.[135]

This asymmetry between cyberattacker and cyberdefender, coupled with the growing vulnerability of today's way of life to cyberattacks, creates one of the most understated

liabilities of the modern age. The risks will undoubtedly increase with the onset of the Internet of Things, which will exponentially raise overall interconnectedness by linking various electronic appliances to the web and therefore substantially increase potential targets for cyberattacks. A precursor of this era of liabilities could be seen with the recall by Fiat Chrysler in July 2015 of up to 1.4 million vehicles because of a vulnerability that could allow hackers to disable them on highways.[136]

A series of high-profile attacks against governments and businesses has brought the issue of cybersecurity to the forefront of public debate. As citizens become increasingly aware that hackers can steal their personal data for malicious purposes, lawmakers have come under pressure to pass legislation that protects the safety and integrity of personal data. Attacks on retailers, banks, health insurers, movie production companies, and even government agencies have highlighted the dearth of cyberprotection and the need to engage in rigorous debates on how to safeguard private information.

The policy response to this growing cybersecurity risk has been twofold. First, governments have developed national plans to enhance their resilience to cyberattacks. These plans include institutional, financial, and scientific measures. Second, policymakers have striven to develop a framework to deter or, failing that, retaliate against cyberattacks. There has been less emphasis on building a set of international norms to reduce the likelihood of cyberattacks or on identifying a generally accepted distinction between cyberattacks and cyberwar.

POLICY POSITIONS

United States

As in many other aspects of the cyberuniverse, the United States has been in the lead in developing a domestic strategy to address cybersecurity. This prominent role is due to the country's huge reliance on digital networks, which affect not only every aspect of the U.S. economy but also its military. In addition, as the world's economic and military superpower, the United States faces constant attacks on its cybernetworks in all industries across all sectors (see box 2).

Box 2: Major Cyberattacks

According to Google's removal request website:

Big retail chains in the United States have been popular targets for hackers due to the wealth of customers' financial information stored in computer databases. In Decem-

ber 2013, Target suffered one of the largest data breaches ever reported, affecting 110 million customer records.[1] In 2014, attackers infiltrated the networks of Michael's in April, Home Depot in September, and Staples in October. Hackers stole tens of millions of customer credit card numbers, and all the companies involved suffered a drastic loss in consumer confidence.[2] Although it is difficult to quantify the cost of cybersecurity breaches, the estimated cost of the breach to Home Depot alone was around $62 million, which included expenses related to credit monitoring and additional staffing at call centers.[3]

The financial sector has also been exposed to the detrimental impact of cyberattacks. In the summer of 2014, cyberattackers siphoned off personal information such as e-mail addresses, home addresses, phone numbers, and checking and savings account information from financial services firm JPMorgan Chase. Over 83 million accounts were compromised.[4]

Some cyberattacks have targeted highly sensitive information like Social Security numbers, such as those of customers of health insurers Community Health Systems and Anthem. In June 2014, the publicly traded hospital operator Community Health Systems suffered a cyberattack that stole the personal data—such as names, birth dates, Social Security numbers, and addresses—of 4.5 million patients.[5] In February 2015, the health insurance provider Anthem suffered a breach in its database, which contained as many as 80 million records of current and former customers as well as employees.[6]

The anonymous nature of cyberattacks allows countries to carry out high-profile attacks with the benefit of having plausible deniability. For example, North Korea is widely believed to have been the perpetrator of attacks in November 2014 against Sony Pictures Entertainment, the company that produced the movie *The Interview*. Hackers leaked e-mails about sensitive topics like contracts, salary lists, and film budgets, causing uproar in the media.

---

1. Nicole Perlroth and David Gelles, "Russian Hackers Amass Over a Billion Internet Passwords," *New York Times*, August 5, 2014, http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html.
2. Joann Weiner, "Despite Cyberattacks at JPMorgan, Home Depot and Target, Many Millennials Aren't Worried About Being Hacked," *Washington Post*, October 8, 2014, https://www.washingtonpost.com/blogs/she-the-people/wp/2014/10/08/despite-cyberattacks-at-jpmorgan-home-depot-and-target-many-millennials-arent-worried-about-being-hacked/.
3. Jim Finkle and Nandita Bose, "Home Depot Breach Bigger Than Target at 56 Million Cards," Reuters, September 18, 2014, http://www.reuters.com/article/us-home-depot-dataprotection-idUSKBN0HD2J420140918.
4. Tanya Agrawal, David Henry, and Jim Finkle, "JPMorgan Hack Exposed Data of 83 Million, Among Biggest Breaches in History," Reuters, October 2, 2014, http://www.reuters.com/article/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003.
5. Dan Munro, "Cyber Attack Nets 4.5 Million Records From Large Hospital System," *Forbes*, August 18, 2014, http://www.forbes.com/sites/danmunro/2014/08/18/cyber-attack-nets-4-5-million-records-from-large-hospital-system/.
6. Anna Wilde Mathews and Danny Yadron, "Health Insurer Anthem Hit by Hackers," *Wall Street Journal*, February 4, 2015, http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720.

Perhaps the most damaging politically motivated and state-sponsored cyberattack to date was the incident in 2014–2015 targeting the U.S. Office of Personnel Management, the human resources department in charge of security clearances for federal agencies. Highly sensitive and personal information for over 21 million current, former, and prospective federal employees was compromised in an effort by China to collect intelligence.

The series of cyberattacks against the department increased the political expediency of developing a more comprehensive framework to address the challenges of cybersecurity both domestically and globally. The White House set up a new cyberunit to oversee the network security of the .gov domain name, including, for the first time, making sure agencies notify victims of breaches according to a specific timetable. Obama's budget proposal for the 2015–2016 fiscal year sought $14 billion for cybersecurity efforts across the U.S. government to better protect federal and private networks from hacking threats. The Pentagon's budget alone called for $5.5 billion in funding for cybersecurity.[137]

The government is also moving beyond defensive measures. The severity of the June 2015 cyberattack against the U.S. Office of Personnel Management forced the Obama administration to consider direct retaliatory action against China. In 2014, five officers of a Chinese army hacking team were indicted on a charge of the theft of intellectual property from U.S. companies. In January 2015, the United States imposed new economic sanctions on North Korean federal agencies and senior officials following a politically motivated cyberattack against U.S. movie production giant Sony Pictures Entertainment.

The prosecution of foreign culprits is part of a more comprehensive response that relies on an assessment of the aims of cyberattacks. According to the U.S. Congressional Research Service, "As a matter of policy, the United States has sought to distinguish between cyber intrusions to collect data for national security purposes—to which the United States deems counterintelligence to be an appropriate response—and cyber intrusions to steal data for commercial purposes—to which the United States deems a criminal justice response to be appropriate."[138]

The more tangible risks associated with cyberspace have led the United States to review its reactionary stance regarding the development of international norms for cybersecurity.

The more tangible risks associated with cyberspace have led the United States to review its reactionary stance regarding the development of international norms for cybersecurity. In a speech to the September 2015 Business Roundtable, an association of U.S. chief executives, Obama stated his desire to see a basic international framework for governments on cybersecurity akin to global nuclear agreements.[139] It is unclear whether Obama's statement reflects a consensus view among U.S. policymakers.

The United States has little willingness to assume leadership on this topic because it is widely believed to use cyberespionage on a major scale with the aim of obtaining political, military, or commercial advantages. Cyberespionage can be defined as the act of stealing secret or confidential information via the Internet. The U.S. government does not deny that it routinely engages in spying to advance American economic advantage, which is part of the government's broad definition of the protection of U.S. national security.

European Union

In 2013, the EU published its first-ever comprehensive strategy on cybersecurity.[140] The document outlined the three main components of EU policy in this area: battling cybercrime, ensuring network and information security, and integrating cybersecurity into the EU's common foreign and defense policies. The EU is expected to adopt in 2016 a new package of measures to improve EU-wide cybersecurity. The package will include additional obligations for operators of essential services and digital service providers. The companies will, for instance, be required to upgrade their cybersecurity resilience and carry out more time-sensitive reporting of cyberattacks. The EU also has a number of internal agencies to develop, manage, and enforce its cybersecurity policy and has taken steps to engage with the international community to address cybersecurity on a global scale.

In the realm of cybercrime, Europol established the European Cybercrime Center in January 2013. Although the center's main aim is to facilitate law enforcement cooperation among EU member states, it is also increasingly becoming a useful tool in cyberdiplomacy. Since its establishment, the center has focused on investigating cybercrimes committed by individuals and groups and has looked into cyberattacks affecting critical infrastructure and information systems in the EU, in addition to supporting training and capacity building.

Bolstering network and information security is the second component of the EU's cybersecurity strategy. To accomplish this goal, the EU has had to work intimately with the private sector to strengthen European defenses against cyberattacks. The European Network and Information Security Agency is the European hub for the exchange of information and knowledge in the field of information security. Established in March 2004, the network deals with cybersecurity threats on the European continent by advising EU member states of information security best practices, collecting and analyzing data on cyberthreats, and promoting awareness and cooperation in defending networks.

To develop and enforce the EU's foreign and defense policies with regard to cybersecurity, the union relies on several internal agencies that handle its foreign and defense policies in general. The European Defense Agency is the EU institution tasked with supporting EU member states' efforts to improve their cyberdefense capabilities. In its capacity as the EU's main foreign, security, and defense policy making body, the European External Action Service promotes the EU's cyberagenda abroad. In addition to internal coordination,

the EU has partnered with other countries and international organizations to enhance cybersecurity. The union has established five bilateral discussion groups with China, India, Japan, South Korea, and the United States and has deepened cooperation with the North Atlantic Treaty Organization (NATO) on a range of issues.

Russia

The Russian state has been leveraging its Soviet heritage of having a scientifically savvy group of hacking experts to lead state-sponsored or state-linked cyberattacks against Western targets.

The Russian state is widely believed to have used cyberattacks for political purposes as well. For years, hackers working for the Russian government have been using sophisticated techniques to break into computer networks, including systems run by Eastern European governments like Georgia and European security organizations like NATO. Of particular visibility were cyberattacks against targets in Estonia in the wake of a 2007 political crisis involving the Russian-speaking minority in the country. In another case, Moscow was widely seen as the culprit behind attacks on Kyrgyzstan in January 2009 aimed at persuading the Kyrgyz president to close down a U.S. military base in the country. Shortly after the attacks stopped, Kyrgyzstan announced plans to close the base and received $2 billion in assistance and loans from Russia.[141]

The Russian state has been leveraging its Soviet heritage of having a scientifically savvy group of hacking experts to lead state-sponsored or state-linked cyberattacks against Western targets.

Russian hackers have also been accused of cyberespionage and systematically targeting hundreds of Western oil and gas companies as well as energy investment firms. Security firms like Symantec, F-Secure, CrowdStrike, and FireEye have tied a string of coordinated attacks on Western oil and gas companies to Moscow. Given the importance of the oil and gas industries to the Russian economy, these cases of industrial espionage were aimed at providing an unfair competitive edge to Russian companies. Hackers reportedly wanted to learn more about competing energy companies' operations, strategic plans, and technologies.[142]

Russian hackers have also developed the know-how to control systems from afar. A December 2014 *Bloomberg Business* article pointed to Russian involvement in an August 2008 explosion on a Turkish oil pipeline, an attack that was originally attributed to the insurgent Kurdistan Workers' Party (PKK).[143] If true, this would be the first example of a cyberattack having a kinetic impact, even before the 2009 release of the Stuxnet computer worm against Iran.

China

China is widely believed to have an active state-sponsored cyberespionage program. Indeed, "China does more in terms of cyberespionage than all other countries put together," said James Lewis, a computer security expert at the Center for Strategic and International Studies.[144]

The Third Department of the General Staff Department of the People's Liberation Army, known as Unit 61398, has received much attention in the West as the alleged perpetrator of a number of high-visibility hacks against Western targets.[145] Although the unit's existence and operations are considered a Chinese state secret, Western intelligence agencies regard it as the hub of China's cyberattacks. Western security services believe that many of the hacking groups located in China are either run by army officers or composed of contractors working for Unit 61398. The unit has been conducting sporadic attacks on U.S. corporate and government computer networks since at least as early as 2006, with some programs that have remained hidden for four years.[146]

The online security company Mandiant has claimed that Unit 61398 has "systematically stolen hundreds of terabytes of data from at least 141 organizations," of which 115 were in the United States.[147] According to Mandiant's list of industries affected by China's cyberespionage activities, most attacks focused on aerospace, satellite technology and telecommunications, and information technology companies that incidentally overlap with the strategic industries earmarked in China's 2011–2015 five-year plan. Mandiant added that the unit "focuses on compromising organizations across a broad range of industries in English-speaking countries" and "maintains an extensive infrastructure of computer systems around the world," and that the size of its infrastructure "implies a large organization with at least dozens, but potentially hundreds of human operators."[148]

In another high-profile case of cyberespionage, Chinese hackers, this time linked to a military unit called the Technical Reconnaissance Bureau, stole vast amounts of sensitive information relating to the F-35 aircraft, including its stealth radar and engine secrets that they later used in the design of their own stealth jet called the J-20.[149]

On the home front, China passed legislation in July 2015 aiming to create a more sophisticated legal framework to address cybersecurity. The national security law formally introduced the concept of cybersovereignty. Article 25 of the law mandates the Chinese government to safeguard the sovereignty and security of its cyberspace and to criminalize various types of cyberattacks.[150] Accordingly, cyberspace is to be considered a contestable space in the struggle for sovereignty akin to physical territory.

Finally, to enhance global cybersecurity, China champions a new international cybersecurity treaty to be negotiated under the aegis of the UN. Like Russia, China considers the

UN the appropriate platform to establish international norms on cybersecurity and codify reasonable standards of state behavior.[151]

POLICY INITIATIVES

International initiatives to develop a multilateral approach to enhance cybersecurity have been hindered by a fundamental divide over the exact role of governments in ensuring cybersecurity. A particularly difficult barrier has been the residual and as yet irreconcilable differences in state policies on human rights, data privacy, and the political uses of the Internet. The non-Western approach has tended to seek to grant governments broad and intrusive powers to improve cybersecurity. This more intrusive method is rejected by Western players, which generally rely on less state-centric and more pluralistic structures. Thus, Western actors have resisted attempts to back treaties formalizing state responsibility at the international level and instead have striven to develop less formal approaches reflecting a more balanced division of labor between government, industry, and civil society. Western governments also resist international cooperation because there is a fear that sharing information about deficiencies in cybersecurity would supply evidence of vulnerabilities that can be used by rivals.

As a result, the two different visions of Western and non-Western governments have produced alternative international approaches. In 2011, China, along with Russia, Tajikistan, and Uzbekistan, submitted to the UN a draft international code of conduct for information security, which they updated in early 2015.[152] This proposal by the members of the Shanghai Cooperation Organization was essentially an attempt to develop interstate cyberconduct norms while recognizing the primary responsibility of national governments to control the Internet to preempt the transformation of this ungoverned space into a security threat. The concept of cybersovereignty embodied in the code of conduct was devoid of appeal to the more liberal members of the international community, which viewed the Chinese-led proposal as paving the way to a legitimization of Internet censorship by authoritarian governments.

A landmark deal that focused exclusively on cybersecurity is the U.S.-Chinese bilateral agreement signed by the two countries' presidents in September 2015.[153] Through the deal, the United States and China took on mutual commitments to refrain from conduct that would be detrimental to each other's cybersecurity. The agreement also covered acts of economic cyberespionage. Although there remain residual difficulties regarding the enforcement of these provisions, the agreement has the potential to create enough momentum to formalize this process at the international level and multilateralize these voluntary commitments. The U.S. president also seemed interested in capitalizing on this opportunity when he said at a meeting with American business leaders in September 2015, "If we and the Chinese are able to coalesce around a process for negotiations, then I think we can bring a lot of other coun-

tries along."[154] A very similar deal was concluded between the UK and China in October 2015.[155] In addition, a comparable objective was incorporated into the declaration issued at the end of the November 2015 G20 summit in Turkey, reflecting a growing sense of awareness among the G20 membership about cybersecurity issues.[156]

For Europe, the anchor deal has been the Council of Europe's 2004 Convention on Cybercrime, commonly referred to as the Budapest Convention, which aims to develop a common criminal-law policy aimed at defining, punishing, and thereby deterring cybercrimes. It serves as the main framework that countries can adopt in formulating their national cybercrime legislation. The convention is open not only to members of the Council of Europe but also to any nation that promises to adhere to the document's principles and recommendations. As of early 2016, 47 states have ratified the convention, including the United States but excluding Russia and China.

TRANSATLANTIC ROAD MAP

As a first step toward a transatlantic agreement on cybersecurity, the partners could continue to push for the universalization of the Budapest Convention. The EU makes its financial support for cybersecurity capacity building in third countries conditional on their signature or broad acceptance of the convention. As part of the U.S. objective of full participation in the development of international cybercrime policy, set out in the 2011 U.S. International Strategy for Cyberspace, the United States has also formally adopted the goal of extending the reach of agreements like the Budapest Convention.

But despite these signs of political willingness, even some like-minded states are missing from the membership list. Conspicuous by their absence are Council of Europe members Greece, Ireland, and Sweden. The convention has only eight non-European members. Canada and South Africa have signed but not ratified the agreement, and Mexico's signature is still pending. The Indian government is critical of the convention as a text that does not sufficiently reflect the positions of developing countries.

Even though they shunned the proposed Chinese-led code of conduct for information security, the United States and the EU could revisit their original stance and explore the feasibility of creating a multilateral instrument more limited in scope but still focused on the prevention of cybercrime. A particularly promising area of potential interstate collaboration could be capacity building for the detection of and forensics related to cyberattacks.[157]

Finally, Brussels and Washington could seek to amend international trade law to introduce a WTO-recognized penalty against the beneficiaries of economic cyberespionage. Such an amendment would address the concerns of corporate entities, which under present rules are unable to redress commercial losses due to cyberespionage.

The difficulty is that a change in the rules of international trade requires the consensus of all WTO members. But the ongoing Trade in Services Agreement negotiations on liberalizing the worldwide trade in services, held under the umbrella of the WTO, could provide an opportunity to advance the agenda of a global response to commercial cyberespionage.

CHAPTER SEVEN

CYBERWAR

Cyberwar offers a novel, unconventional method of military conflict. As such, it can be seen as the newest frontier of warfare, extending the known universe of land, air, sea, and space. Cyberwar needs to be differentiated from cybercrime, which covers non-state-sponsored, illegal actions at either the national or the international level.

From the execution of routine procedures like bank transfers to the monitoring and management of critical infrastructure such as oil pipelines or power grids, increased reliance on the Internet means that nations' vulnerabilities to cyberattacks have also increased. Liberal Western democracies, by virtue of having the most connected societies, are the ones most vulnerable to cyberattacks and cyberwar.

The overall understanding of the concept and consequences of cyberconflicts is still at an early stage. Many parallels are drawn between cyberwarfare and the dawn of the nuclear age. Kennette Benedict, the former executive director and publisher of the *Bulletin of the Atomic Scientists*, argued, "We have come to know how nuclear weapons can destroy societies and human civilization. We have not yet begun to understand how cyberwarfare might destroy our way of life."[158]

The international community has started to address and build consensus on some of these critical themes. There is a commonly agreed definition of what constitutes cyberwar. According to a report drafted by independent experts under UN auspices, cyberwar occurs

when the "level of damage inflicted was similar to an armed attack."[159] There is also overall agreement that to be classed as a cyberattack, an incident has to conform to the major principles of the law of armed conflict and international humanitarian law, but little progress has been made beyond these basic tenets.

States need primarily to establish mechanisms of interaction in cyberspace to prevent unwanted escalations in situations of cyberconflict. Governments need clearer rules to determine the scope of legitimate responses to cyberattacks. Specifically, determining when a cyberattack meets the UN Charter's criteria for an armed attack and assessing whether such an attack warrants UN-sanctioned self-defense are key issues that so far have remained unaddressed. For instance, can a state invoke its right of retaliation under Article 51 of the UN Charter if there is an identifiable and state-sponsored cyberattack against one of its commercial banks or against its critical infrastructure? For that matter, what should be the definition of critical infrastructure that needs to be protected against cyberattacks?

Governments need clearer rules to determine the scope of legitimate responses to cyberattacks.

Cyberattacks should be defined to discriminate between military and civilian targets and comply with the proportionality principle, which is used to judge the lawfulness of an armed attack. In this respect, one particular challenge relates to attribution. It is immensely more difficult in a cyberconflict than in a conventional conflict to unambiguously determine the identity of the belligerent; and without this identification, governments cannot develop appropriate response strategies. A related difficulty is the definition of a state's responsibility for preventing its territory from being used for cyberattacks by non-government-affiliated entities.

New rules for containing cyberconflict also have to be devised to avoid unforeseen consequences of an attack. A particular focus will be on collateral damage. Modern military technology allows a very precise determination of possible collateral damage in conventional warfare. The development of satellite and drone technologies, combined with precision-guided smart weapons, is helping military planners to determine quite precisely the expected damage of an attack on civilian populations, but cyberwarfare lacks such constraints. The launch of a cyberweapon targeting an adversary's online capabilities can easily damage civilian infrastructure as well. Unlike conventional or nuclear weapons, cyberweapons have unique capabilities of replication and dissemination. As a result, military planners cannot know in advance the scale and scope of the destruction unleashed by a cyberweapon. That is also an argument for the creation of new rules for the cyberworld akin to the disarmament treaties that exist for conventional and nuclear weapons.

Failure to work toward such common norms of appropriate behavior in cyberspace opens the door to a deeply uncertain security environment in which cyberconflicts can easily escalate and degenerate into full-scale military confrontations.

POLICY POSITIONS

United States

The United States was the first Western nation to fully embed the concept of cyberwar in its military strategy and doctrine. In 2009, the U.S. Cyber Command, a military headquarters designed to coordinate the Pentagon's efforts on cyberwar and computer-network security, was set up, and General Keith Alexander, a former NSA director, was nominated to lead it. The White House's 2015 National Security Strategy emphasized cyberthreats, stating that "the danger of disruptive and even destructive cyber-attack is growing."[160] With an annual budget exceeding $3 billion, the U.S. Cyber Command was to have a staff of 6,000 by the end of 2015.[161]

In addition to building up the resilience of its critical assets against cyberattacks, the United States has been intent on enhancing its offensive capabilities. In 2013, the CIA received $685 million, the NSA $1 billion, and the U.S. Cyber Command $4 billion in U.S. government funding to carry out offensive cyberoperations and develop spyware that could be used against countries regarded as unfriendly to the United States, specifically China, Iran, North Korea, and Syria.[162]

Being an early responder to cyberthreats with formidable human, technical, and financial resources has led the United States to adopt an uncooperative approach to cyberwar discussions. The belief among U.S. policymakers has been that the United States had the first-mover advantage and had built up capabilities, including offensive capabilities, that other parties would have difficulty in matching or replicating. This large gap between U.S. capabilities and those of the rest of the world would act as a deterrent against cyberattacks—or so Washington believed. Therefore, U.S. goals would be better served by eschewing discussions about cyberweapons and maintaining a noncommittal position.

Another reason for this strategy of ambiguity was the inadequacy of international law on cyberwarfare. U.S. policymakers had to be cautious as their responsibility for having developed and possibly launched cyberweapons was ill-defined from the standpoint of international law. With Stuxnet and accompanying U.S.-attributed cyberwarfare programs, the United States has gained the reputation of having initiated the era of state-to-state cyberwarfare.[163] The United States, in cooperation with Israel, is believed to be the designer of the computer virus and the originator of the attack against Iran's nuclear program. But neither U.S. nor Israeli policymakers have ever publicly taken responsibility for this successful operation. At the time it was uncovered, Stuxnet was the first known government-

sponsored cyberweapon that had a kinetic impact, having caused malfunctions and even destroyed a set of physical installations—enrichment centrifuges—of critical value to Iran's nuclear enrichment program. According to the *New York Times*, U.S. officials credit Stuxnet and its associated program, Olympic Games, with having delayed Iran's progress toward a nuclear-weapon capability by a year and a half to two years.[164]

Washington opposed any formal multilateral disarmament-like negotiations related to cyberwarfare, a position that discouraged NATO from adopting a more ambitious offensive approach to complement the alliance's effort to develop defensive capabilities in this area.

However, in the wake of a number of well-advertised cyberattacks against U.S. targets, the Obama administration seems to have been compelled to reevaluate its position on cyberdeterrence. Commenting on the administration's response to the theft by hackers associated with the Chinese government of the personal information of more than 21 million Americans from the database of the U.S. Office of Personnel Management, an unnamed member of the administration said, "One of the conclusions we've reached is that we need to be a bit more public about our responses, and one reason is deterrence," according to the *New York Times*.[165] In addition, for deterrence to be effective in cyberspace, more clarity would be needed on thresholds for retaliation. Potential adversaries should know in advance the scale and scope of expected retaliation. Otherwise, cyberattacks cannot be deterred simply by the threat of retaliation. Therefore, more public clarity on the U.S. cyberdeterrence doctrine could promote stability by shaping other parties' expectations of U.S. behavior.

This reassessment is likely to lead to a change in the U.S. posture on cyberdeterrence, with more information starting to become publicly available about the country's offensive capabilities and about the prevailing doctrine on retaliation against cyberattacks.[166] The 2015 Department of Defense Cyber Strategy underlined the importance of declaratory policy for better deterrence and reiterated the U.S. position that "the United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law."[167] Such a change in U.S. posture could also lead to the development of a more ambitious set of objectives and capabilities for the Atlantic alliance.

Russia and China

In relation to the development of international norms for cyberwarfare, Russia and China have very similar viewpoints. They are both heavily influenced by the perceived technological superiority of the United States and its companies' online predominance, which is viewed as a threat by both authoritarian regimes. China has also accused the United States of militarizing cyberspace and triggering an international cyberarms race.[168] As a result, the Chinese government has adopted a declaratory cyberwar policy by confirming that Beijing will retaliate if faced with a cyberattack.[169]

This perceived power asymmetry in cyberspace has led the Russian and Chinese governments to establish their own resources, including offensive cyberwarfare capabilities. At the international level, Moscow and Beijing have been at the forefront of calls to establish an international regime for cyberspace disarmament. Such a regime would seek to ban the development and deployment of cyberweapons. To further consolidate their common position at the international level, Russia and China signed a treaty in May 2015 that can be interpreted as a bilateral arms control agreement for cyberspace. Through the accord, the two countries have taken on an obligation to refrain from engaging in cyberconflict with each other.

POLICY INITIATIVES

The UN has been a critical platform for the development of key concepts and norms related to cyberwarfare, relying on a series of meetings by a group of governmental experts on information security to develop these concepts. The first such meeting on the topic of information security was held in 2004 at the suggestion of Russia. Since then, three more meetings have been held. The process was given additional recognition by a unanimously adopted 2013 UN General Assembly resolution that took note of the outcome of the 2012–2013 meeting and requested that the UN secretary general establish a new group that would report to the General Assembly in 2015.[170] The group's 2014–2015 meetings produced an important consensus document on "norms, rules or principles of the responsible behaviour of States in the cyber-sphere as well as confidence building measures, international cooperation and capacity building which could have wider application to all States."[171] The main conclusions of the report, which was presented in October 2015 to the General Assembly's Disarmament and International Security Committee, were as follows:

> In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms. . . .
>
> States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts. . . .
>
> The United Nations should play a leading role in promoting dialogue on the security of ICTs in their use by States and developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour.[172]

A number of authoritarian states used the UN platform to launch a proposal for an international code of conduct for information security. Co-sponsored by China, Rus-

sia, Tajikistan, and Uzbekistan, the proposal was circulated in a 2011 letter to the UN secretary general. Although the plan did not set out detailed rules, it nonetheless aimed to introduce a negative security assurance by obliging contracting parties to refrain from launching cyberattacks:

> Each State voluntarily subscribing to the code pledges . . . not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies.[173]

The ITU also aimed to contribute to this emerging debate by launching its Global Cybersecurity Agenda. In an effort to define cyberpeace, ITU Secretary General Hamadoun Touré underlined in 2011 the agenda's five key principles:

- Every government should commit itself to giving its people access to communications.
- Every government should commit itself to protecting its people in cyberspace.
- Every country should commit itself not to harbour terrorists / criminals in its own territories.
- Every country should commit itself not to be the first to launch a cyberattack on other countries.
- Every country should commit itself to collaborate with others within an international framework of co-operation to ensure that there is peace in cyberspace.[174]

The Organization for Security and Cooperation in Europe (OSCE) has been among the international institutions that have contributed to making norms in this field. In 2013, the organization produced a set of concrete proposals branded as confidence-building measures to reduce the risks of conflict stemming from the use of ICT. This list portrayed the OSCE as a dialogue platform for a regular exchange on cybersecurity issues.[175]

In addition, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* is the outcome of a NATO-sanctioned effort by independent experts to examine how existing international humanitarian law applies to cyberwarfare. Published in 2013, the manual addressed topics including sovereignty, state responsibility, the right to war, international humanitarian law, and the law of neutrality. The departure point of the manual is that cyberwarfare is governed by international law already in force, particularly the rules that regulate the commencement of an armed attack and the conduct of armed conflict.[176] Since the manual was published, the group that drafted the document has continued its work, focusing on the concept of state responsibility in cyberattacks. As of early 2016, the experts are "attempting to develop a consensus around how the law of state responsibility applies to the use of proxies in cyber operations," according to the Council on Foreign

Relations.[177] The understanding is that states need to be held accountable for actions originating from within their borders. The new provisions to be included in an updated version of the manual aim to clarify the responsibility of states to monitor their networks and prevent malicious cyberattacks.

TRANSATLANTIC ROAD MAP

Despite a number of different multilateral and regional diplomatic efforts to promote the development of shared norms and expectations regarding cyberwarfare, the emergence of an overall consensus on state behavior is unlikely in the near future due to the diversity of national interests, capabilities, and assessments of threats and vulnerabilities. But efforts to build common norms can instead focus on a scaled-down accord that defines agreed constraints on the use of cyberweapons. Beyond identifying targets such as medical services that are normally immune from conventional attacks during armed conflict, governments could also agree to extend the umbrella of protection from cyberattacks to other critical nodes such as power grids, air and road traffic control, food supplies, and financial infrastructure.

Given the resistance of the United States to a multilateral code of conduct—which U.S. policymakers view as an unenforceable and therefore impractical objective—deliberations on mutually agreed redlines in cyberconflict can at this stage best be advanced by way of high-level bilateral talks.[178] The various bilateral diplomatic platforms devoted to topics in this area—such as the cybersecurity working groups between the United States and China or between the United States and Russia, as well as the summits held between the United States and the EU—should be used to advance this key agenda. Also, to quote Richard Danzig of the Center for a New American Security and a former senior adviser to Obama on national security issues, "An agreement with either country could pave the way for agreement with the other and facilitate other cooperative efforts to limit destructive cyber attacks involving other nations and subnational groups."[179]

Efforts to build common norms can focus on an accord that defines agreed constraints on the use of cyberweapons.

One area that should be explored in this context is the case of zero-day exploits. These exploits begin as software weaknesses that developers have not yet corrected because they are not publicly known. The weaknesses are discovered by third parties that then develop cyberweapons to exploit them. It is claimed that Stuxnet used at least four such zero-day exploits, one being a weakness in Microsoft Windows.[180]

The utility of zero-day exploits for cyberattacks has spawned both demand and supply. On the supply side, it was estimated that at the beginning of the 2010s, more than 30,000

vulnerability analysts were offering their expertise at the global level.[181] On the demand side, a myriad of actors ranging from intelligence agencies to crime syndicates to concerned producers is interested in the acquisition of this knowledge. Markets even exist on which these exploits are bought and sold.

But the use of zero-day attacks presents an ethical problem for governments. Once governments acquire knowledge of the specific vulnerabilities of widely used software products, should they be allowed to keep this critical information to themselves at the cost of maintaining the vulnerability and continuing to expose users to such attacks? Or should they share this knowledge with the software developer so that patches can be quickly developed and distributed to address the weakness?

The risks of proliferation posed by the nonregulation of the use of zero-day exploits should move governments to develop a set of norms that would at least seek to criminalize the sale of zero days and impose limitations on governments regarding their exploitation.[182]

Incidentally, constraining the use of zero-day exploits was on the list of recommendations of the surveillance reform board set up by the White House in the wake of the Snowden revelations. The board's report recommended that the U.S. National Security Council establish a process for reviewing the U.S. government's use of zero-day exploits. "US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks," stated the report, which also noted that "in rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection."[183]

From a transatlantic perspective, the partners should overhaul the role of NATO in this area and, especially, revisit the alliance's policy on cyberdeterrence. NATO is already involved in cyberwarfare discussions. Following cyberattacks in 2007 against NATO ally Estonia, which accused Russia of being responsible, the alliance was urged to develop a concept of cyberdefense. This momentum culminated with NATO's 2010 Lisbon summit and Strategic Concept, in which the allies declared for the first time their posture on cyberwar. The summit declaration urged NATO to accelerate efforts to respond to the danger of cyberattacks. The Strategic Concept indirectly addressed the issue of whether NATO's Article 5 mutual defense clause applied to cyberspace, with the allies reiterating the principle of collective defense for all categories of threats, including cyberattacks. The Strategic Concept also called for the introduction of cyberdeterrence in the alliance's defense-planning process. In 2008, NATO set up a Cooperative Cyber Defense Center of Excellence in Tallinn to help build capacity and share information among NATO allies on cybersecurity and cyberdefense.

Despite these efforts, to date, the U.S. resistance to discussing cyberdeterrence, including offensive capabilities, even with its allies has limited NATO's remit to defense. The U.S.

secrecy about offensive capabilities "has carried over into NATO, and is unhelpful in that it increases the likelihood of opponents miscalculating as they consider the risks of using force or coercion against NATO members or interests," according to James Lewis in a paper published by NATO's Cyber Defense Center of Excellence.[184]

Yet, the recent proclivity to bring more clarity to the U.S. position on these issues can now be leveraged to give NATO a more ambitious mandate. An agreement on a more ambitious NATO posture on cyberpolicy—possibly defining cyberspace as a new operational theater in addition to land, sea, and air—could be achieved at NATO's 2016 Warsaw summit. NATO can then develop a more cogent and robust approach for cyberdeterrence. This would imply a debate about the use of offensive capabilities on behalf of the alliance. Lewis argued that "adding offensive cyber capabilities to NATO's force structure and response doctrine will increase its deterrent capabilities."[185] Such a decision would trigger new planning challenges as the cyberdimension would need to be integrated more thoroughly into strategic and tactical military planning. A related challenge will be to devise—just as in the nuclear field with the NATO Nuclear Planning Group—rules for the the sharing of cyberwarfare capabilities at a time when only a few allies are endowed with such assets.

CHAPTER EIGHT

A ROAD MAP FOR TRANSATLANTIC CYBERPOLICY LEADERSHIP

In the realm of cyberspace, modern-day equivalents of King Philip VI of France are not difficult to find. The world has seldom faced such a fast transition to a new order while also being so oblivious to the full range of its consequences. Leaders in government and business are just beginning to understand the ramifications of an interconnected digital world. From the German chancellor whose private phone conversations were tapped, to the director of the U.S. Office of Personnel Management who was not able to prevent hackers from stealing more than 21 million personnel records, to the owner of the local bookstore who had to close shop due to competition from Internet giants like Amazon, a sense of inescapability is brewing.

And yet, policymaking has been greatly outpaced by this technology-driven dynamic. In that sense, the emergence of an omnipresent cyberreality can perhaps best be compared with the dawn of the nuclear age, when policy followed technology after a decade. But unlike the nuclear realm, technologies in the digital world lack inherent barriers to proliferation. The world had only two nuclear powers a decade after the first use of nuclear weapons. Today, many governments as well as nonstate actors have developed tools of cyberwarfare, including espionage and offensive capabilities. A failure to advance a global framework for cyberpolicy is therefore likely to have adverse short-term consequences for humanity.

Unlike other areas of the global commons, however, cyberpolicy escapes any simplistic effort to categorize national preferences, as there is a lack of overlap even among liberal

democracies. In international trade, by contrast, Western powers have acted first as norm makers and then as the lynchpin of the international order. The West has been at the vanguard of continuing initiatives to liberalize global trade. Differences among Western actors and between the EU and the United States have been real but not systemic. These divergences have not posed a challenge to the continuation of prevailing rules. Among non-Western countries, China is gradually emerging as an influential player by participating in the exercise of setting norms. On climate change, the EU led an effort to establish a lasting international regime with binding commitments to mitigate greenhouse gas emissions, an effort the United States joined belatedly. Emerging nations like China and India have been more willing to take on commitments to support the emergence of a global set of norms.

Cyberpolicy does not lend itself to such categorizations. One reason it is difficult to categorize is that international norms related to cyberspace are sparse. Another reason is that leadership and collective action for the development of these norms has been lacking. The weakness of international governance of cyberspace stands in stark contrast to the accelerating pace of challenges, which follow the curve of technological innovation and its dissemination. The paucity of multilateral rules is an indication of a lost opportunity to create a more prosperous but also less volatile and more secure international environment.

The weakness of international governance of cyberspace stands in stark contrast to the accelerating pace of challenges.

Given the economic and technological edge of the United States and Europe in this area, the transatlantic partners have a natural interest in seeking to play a more influential role in the emerging debate on norms to govern cyberspace. The willingness of leaders in Washington and Brussels plays a bigger role in influencing cyberpolicies and is to be welcomed. In 2011, the U.S. government's International Strategy for Cyberspace set out an ambitious vision for the making of global policy to govern cyberspace, with references to the protection of the freedom of expression online, the promotion of innovation, support for the multistakeholder model of Internet governance, and the prevention of cyberattacks and cybercrime. The EU's Cybersecurity Strategy of 2013 advises the union to establish a coherent international cyberspace policy including deepened dialogue with like-minded third countries. Both the United States and the EU have tentatively initiated a diplomatic track for cyberpolicy and have started to engage third countries on cyberpolicy issues.

The impact of these disparate attempts can be greatly enhanced by a more robust U.S.-EU joint effort to advance a more ambitious cyberpolicy framework at the global level.

The feasibility of such an initiative will in turn depend on the possibility of convergence between Washington and Brussels in the key policy areas related to cyberspace.

Although the United States and the EU may display divergent interests and positions on some key topics, there is also a significant degree of real and potential convergence. In particular, the development of norms on government-industry collaboration on access to online data, the elaboration of a new multilateral instrument to prevent cybercrime, the amendment of international trade law to introduce penalties for economic cyberespionage, the codification of norms for the export of surveillance technologies, and a NATO mandate to develop a more robust approach to cyberdeterrence represent areas where existing transatlantic policy convergence can be leveraged to greatly impact policy shaping the cyberworld (see table 2). This observation should be the basis for Washington and Brussels to prioritize a new approach for joint diplomacy aimed at creating a global policy framework for cyberspace.

History has amply demonstrated the costs of failed policy leadership in times of crisis or fundamental transformation—from the containment policies of the years before World War II to the current tragedy of refugees fleeing war-torn countries in the Middle East. In all of these cases, the United States and Europe have failed to act in unison or have done so only belatedly. Cyberspace is the next frontier, the next global commons that can be shaped to the advantage of future generations, if only there were a joint sense of policy entrepreneurship that would further cement the transatlantic alliance.

Table 2: **Likelihood and Global Impact of U.S.-EU Convergence on Key Cyberpolicies**

POLICY THEME	LIKELIHOOD OF U.S.-EU CONVERGENCE	GLOBAL IMPACT OF U.S.-EU CONVERGENCE
ONLINE SURVEILLANCE	**1**	**2**
Introduce norms on government-industry collaboration for access to online data	**2**	**3**
Increase government-to-government collaboration for the sharing of online data	**3**	**2**
Develop an international instrument requiring the respect of data protection standards by intelligence activities	**1**	**2**
FREEDOM OF EXPRESSION ONLINE	**3**	**3**
Support the Global Network Initiative	**3**	**1**
Expand the Freedom Online Coalition	**3**	**2**
Elaborate norms for export of surveillance technologies	**3**	**3**
CROSS-BORDER DATA FLOWS	**1**	**3**
Liberalize cross-border data flows with TTIP	**1**	**3**
Strengthen the Safe Harbor arrangement	**3**	**1**
Develop interoperable mechanisms among different privacy regimes	**1**	**3**

Legend: **1** LOW; **2** MEDIUM; **3** HIGH

Source: Author's evaluation

POLICY THEME	LIKELIHOOD OF U.S.-EU CONVERGENCE	GLOBAL IMPACT OF U.S.-EU CONVERGENCE
INTERNET GOVERNANCE	**3**	**2**
Empower ICANN's Government Advisory Council	**3**	**1**
Strengthen the Internet Governance Forum	**3**	**1**
ELECTRONIC COMMERCE	**2**	**1**
Get a permanent and binding moratorium on customs duties on electronic communications	**3**	**1**
Jointly seek more liberal commitments under TiSA in e-commerce-related policy areas	**3**	**1**
CYBERSECURITY	**2**	**3**
Push for the universalization of the Budapest convention on cybercrime	**3**	**3**
Create a multilateral instrument to prevent cybercrime	**2**	**3**
Amend international trade law to introduce a penalty for economic cyberespionage	**3**	**2**
CYBERWAR	**2**	**3**
Create an instrument to constrain the use of zero-day exploits	**1**	**2**
Allow NATO to develop a more robust approach to cyberdeterrence	**2**	**3**

NOTES

1 Jack Gillum, "NSA Winning Internet Security War, Reports Show," *Huffington Post*, September 5, 2013, http://www.huffingtonpost.com/2013/09/05/nsa-internet-security_n_3876309.html.

2 European Parliament, Study by the Directorate General for Internal Policies PE 493.032, "National Programmes for Mass Surveillance of Personal Data and Their Compatibility with EU Law," October 2013, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf.

3 "Toward a Social Compact for Digital Privacy and Security," statement by the Global Commission on Internet Governance, Centre for International Governance Innovation and Chatham House, April 15, 2015, https://www.ourinternet.org/publication/toward-a-social-compact-for-digital-privacy-and-security/.

4 Robert Hannigan, "The Web Is a Terrorist's Command-and-Control Network of Choice," *Financial Times*, November 3, 2014, http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3uboyrr6O.

5 Ben Quinn, "UK Surveillance Bill Could Bring 'Very Dire Consequences,' Warns Apple Chief," *Guardian*, November 9, 2015, http://www.theguardian.com/world/2015/nov/10/surveillance-bill-dire-consequences-apple-tim-cook.

6 For more detailed information, see Stefan Heumann and Ben Scott, "Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany," Stiftung neue verantwortung and Open Technology Institute of the New America Foundation, September 30, 2013, http://www.stiftung-nv.de/publikation/law-and-policy-internet-surveillance-programs-united-states-great-britain-and-germany.

7 Daniel Castro, "How Much Will PRISM Cost the U.S. Cloud Computing Industry," Information Technology and Innovation Foundation, August 5, 2013, http://www2.itif.org/2013-cloud-computing-costs.pdf?_ga=1.136613936.1838271416.1445954273; James Staten, "The Cost of

PRISM Will Be Larger Than ITIF Projects," Forrester, August 14, 2013, http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

8 Cameron Kerry, "Missed Connections: Talking With Europe About Data, Privacy, And Surveillance," Center for Technology Innovation, Brookings Institution, May 2014, http://www.brookings.edu/~/media/research/files/papers/2014/05/20-europe-privacy-surveillance-kerry/kerry_europefreetradeprivacy.pdf.

9 Ibid.

10 *Big Data: Seizing Opportunities, Preserving Values* (Washington: Executive Office of the President, May 2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

11 European Commission, MEMO/13/923, "LIBE Committee Vote Backs New EU Data Protection Rules," October 22, 2013, http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.

12 Annegret Bendiek, "Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection," SWP Research Paper, Stiftung Wissenschaft und Politik, March 2014, http://www.swp-berlin.org/fileadmin/contents/products/research_papers/2014_RP05_bdk.pdf.

13 European Court of Human Rights, "Third Section Decision as to the Admissibility of Application No. 54934/00 by Gabriele Weber and Cesar Richard Saravia Against Germany," June 29, 2006, http://hudoc.echr.coe.int/eng#{"itemid":["001-76586"]}.

14 The following minimum safeguards were highlighted: first, the nature of the offenses that may give rise to an interception order; second, a definition of the categories of people liable to have their telephones tapped; third, a limit on the duration of telephone tapping; fourth, the procedure to be followed for examining, using, and storing the data obtained; fifth, the precautions to be taken when communicating the data to other parties; and sixth, the circumstances in which recordings may or must be erased or the tapes destroyed. European Parlaiment, "National Programmes for Mass Surveillance," 2013.

15 "Gabriele Weber and Cesar Richard Saravia Against Germany," European Court of Human Rights, 2006.

16 Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," *World Policy Journal* 30, no. 3 (Fall 2013), http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

17 Scott Livingston, "Beijing Touts 'Cyber-Sovereignty' in Internet Governance: Global Technology Firms Could Mine Silver Lining," *China Law Blog*, February 19, 2015, http://www.chinalawblog.com/2015/02/beijing-touts-cyber-sovereignty-in-internet-governance-global-technology-firms-could-mine-silver-lining.html.

18 Paul Carsten, "China Drops Leading Tech Brands for Certain State Purchases," Reuters, February 27, 2015, http://www.reuters.com/article/us-china-tech-exclusive-idUSKBN0LV08720150227.

19 Cory Bennett, "China Wants Cyber 'Sovereignty' in Latest National Security Law," *Hill*, May 8, 2015, http://thehill.com/policy/cybersecurity/241420-china-wants-cyber-sovereignty-in-latest-national-security-law.

20 United Nations General Assembly, Resolution No. 68/167, "The Right to Privacy in the Digital Age," December 18, 2013, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167.

21 Office of the United Nations High Commissioner for Human Rights (OHCHR), A/HRC/27/37, "The Right to Privacy in the Digital Age," June 30, 2014, http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

22 European Parliament, "National Programmes for Mass Surveillance," 2013.

23 OHCHR, "The Right to Privacy in the Digital Age," 2014.

24 Organisation for Economic Co-operation and Development, C(80)58/FINAL, "OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," July 11, 2013, http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

25 "Core Commitments," Global Network Initiative, accessed December 12, 2015, http://www.globalnetworkinitiative.org/corecommitments/index.php.

26 Richard Fontaine and Will Rogers, *Internet Freedom: A Foreign Policy Imperative in the Digital Age* (Washington: Center for a New American Security, June 2011), http://www.cnas.org/files/documents/publications/CNAS_InternetFreedom_FontaineRogers_0.pdf.
27 Edward Wyatt and Claire Cain Miller, "Tech Giants Issue Call for Limits on Government Surveillance of Users," *New York Times*, December 9, 2013, http://www.nytimes.com/2013/12/09/technology/tech-giants-issue-call-for-limits-on-government-surveillance-of-users.html.
28 Ibid.
29 "Toward a Social Compact for Digital Privacy and Security," 2015.
30 Ibid.
31 Ibid.
32 Ibid.
33 Rebecca MacKinnon, "The Ranking Digital Rights 2015 Corporate Accountability Index Is Now Online," Ranking Digital Rights, November 3, 2015, https://rankingdigitalrights.org/2015/11/03/index-now-online/.
34 "About the Project," Ranking Digital Rights, accessed December 12, 2015, https://rankingdigitalrights.org/about/.
35 Murad Ahmed and Richard Waters, "Microsoft Unveils German Data Plan to Tackle US Internet Spying," *Financial Times*, November 11, 2015, http://www.ft.com/intl/cms/s/0/540a296e-87ff-11e5-9f8c-a8d619fa707c.html.
36 A similar recommendation is included in a Council of Foreign Relations Independent Task Force Report. See John D. Negroponte, Samuel J. Palmisano, and Adam Segal, *Defending an Open, Global, Secure, and Resilient Internet*, Independent Task Force Report No. 70 (New York: Council on Foreign Relations, 2013), http://www.cfr.org/cybersecurity/defending-open-global-secure-resilient-internet/p30836.
37 For a similar recommendation, see "Toward a Social Compact for Digital Privacy and Security," 2015.
38 European Court of Justice, "Judgment of the Court in Joined Cases C-293/12 and C-594/12," April 8, 2014, http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN.
39 United States Court of Appeals for the Second Circuit, "ACLU v. Clapper, Case 14-42, Document 168-1," May 7, 2015, https://www.aclu.org/sites/default/files/field_document/clapper-ca2-opinion.pdf.
40 European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on 'Rebuilding Trust in EU-US Data Flows' and on the Communication From the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour From the Perspective of EU Citizens and Companies Established in the EU," February 20, 2014, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-02-20_EU_US_rebuliding_trust_EN.pdf.
41 Mark Robertson, "300+ Hours of Video Uploaded to YouTube Every Minute," ReelSEO, November 21, 2014, http://www.reelseo.com/youtube-300-hours/.
42 European Court of Justice, "Judgement of the Court in Case C-131/12," May 13, 2014, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=277360#Footnote*.
43 "Search Removal Request Under Data Protection Law in Europe," Google, 2015, https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=en.
44 Rory Cellan-Jones, "US v Europe – A Cultural Gap on the Right to Be Forgotten," BBC, May 15, 2014, http://www.bbc.com/news/technology-27421969.
45 Michael Birnbaum, "Russian Blogger Law Puts New Restrictions on Internet Freedoms," *Washington Post*, July 31, 2014, http://www.washingtonpost.com/world/russian-blogger-law-puts-new-restrictions-on-internet-freedoms/2014/07/31/42a05924-a931-459f-acd2-6d08598c375b_story.html.
46 Ibid.

47 Shaun Walker, "Russian Data Law Fuels Web Surveillance Fears," *Guardian*, September 1, 2015, http://www.theguardian.com/world/2015/sep/01/russia-internet-privacy-laws-control-web.
48 Scott D. Livingston, "Beijing Touts 'Cyber-Sovereignty' in Internet Governance," *China File*, February 19, 2015, http://www.chinafile.com/reporting-opinion/viewpoint/beijing-touts-cyber-sovereignty-internet-governance.
49 Glyn Moody, "Is Facebook Censoring Posts to Please China?" *Techdirt*, January 8, 2015, https://www.techdirt.com/articles/20150106/03023529604/is-facebook-censoring-posts-to-please-china.shtml.
50 Ian Johnson, "Facebook Blocks Account of Liao Yiwu, Exiled Chinese Writer," *Sinosphere* (blog), *New York Times*, December 31, 2014, http://sinosphere.blogs.nytimes.com/2014/12/31/facebook-blocks-account-of-liao-yiwu-exiled-chinese-writer/.
51 Cindy Chiu, Chris Ip, and Ari Silverman, "Understanding Social Media in China," McKinsey Quarterly, April 2012, http://www.mckinsey.com/insights/marketing_sales/understanding_social_media_in_china.
52 Sonya Song, Rob Faris, and John Kelly, "Beyond the Wall: Mapping Twitter in China," Berkman Center for Internet and Society, Harvard University, November 4, 2015, https://cyber.law.harvard.edu/publications/2015/beyond_the_wall.
53 Ayatollah Khamenei has multiple official Twitter accounts in different languages, including Farsi, English, French, and Spanish. The English language Twitter account can be found here: https://twitter.com/khamenei_ir?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor.
54 Sam Wilkin and Mehrdad Balali, "Iran's Guards Increase Monitoring of Social Media: State TV," Reuters, March 3, 2015, http://www.reuters.com/article/2015/03/03/us-iran-internet-idUSKBN-0LY1YC20150303.
55 Ibid.
56 "Iran's 'Smart Filter' for Internet Now in Second Stage," Radio Zamaneh, July 25, 2015, http://en.radiozamaneh.com/featured/irans-smart-filter-for-internet-now-in-second-stage/.
57 United Nations Human Rights Council, A/HRC/17/27, Seventeenth session, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," May 16, 2011, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
58 The Facebook document is entitled "Government Requests Report." See "Government Requests Report," Facebook, 2015, https://govtrequests.facebook.com.
59 Turkey has made by far the most removal requests, at 718, amounting to more than 70 percent of the total. "Transparency Report: Removal Requests," Twitter, accessed December 12, 2015, https://transparency.twitter.com/removal-requests/2015/jan-jun.
60 "Google Transparency Report: Government Requests to Remove Content," Google, accessed December 16, 2015, https://www.google.com/transparencyreport/removals/government/?hl=en.
61 "Transparency Report: Removal Requests," Twitter, accessed December 21, 2015, https://transparency.twitter.com/removal-requests/2015/jan-jun.
62 "Community Guidelines," YouTube, accessed December 15, 2015, http://www.youtube.com/yt/policyandsafety/communityguidelines.html.
63 "Abusive Behavior Policy," Twitter, accessed December 15, 2015, https://support.twitter.com/articles/20169997.
64 "Community Standards," Facebook, accessed December 15, 2015, https://www.facebook.com/communitystandards#.
65 "About Us," Freedom Online Coalition, accessed December 12, 2015, https://www.freedomonlinecoalition.com/about/.
66 Ministers of the Freedom Online Coalition, "Recommendations for Freedom Online," Freedom Online Coalition, April 28, 2014, https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf.

67 J.M. Berger and Jonathon Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," Analysis Paper No. 20, Brookings Project on U.S. Relations with the Islamic World, March 2015, http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

68 Rick Gladstone, "Twitter Says It Suspended 10,000 ISIS-Linked Accounts in One Day," *New York Times*, April 9, 2015, http://www.nytimes.com/2015/04/10/world/middleeast/twitter-says-it-suspended-10000-isis-linked-accounts-in-one-day.html.

69 One anti–Islamic State activist, who goes by the Twitter user name JewHadi, said that many suspended users reestablish accounts within twenty-four hours, making only slight modifications to their suspended user name by simply adding a number or a letter. One of these accounts, turjuman, has apparently been suspended 122 times and is now on its 123rd iteration.

70 White House "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

71 High Representative of the European Commission for Foreign Affairs and Security Policy, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," July 2, 2013, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

72 Council of the European Union, 6122/15, "Council Conclusions on Cyber Diplomacy," February 11, 2015, http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

73 The United States and setup has held cyberpolicy specific bilateral meetings with India, Brazil, South Africa, South Korea, Japan, and Germany. The EU has established cyberpolicy relevant task forces and dialogues with China, India, Brazil, Japan, Russia, South Africa, and South Korea.

74 James Manyika et al., "Big Data: The Next Frontier for Innovation, Competition, and Productivity," McKinsey Global Institute, May 2011, http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

75 James Manyika et al., "Global Flows in a Digital Age," McKinsey Global Institute, April 2014, http://www.mckinsey.com/insights/globalization/global_flows_in_a_digital_age.

76 Susan Stone, James Messent, and Dorothee Flaig, *Emerging Policy Issues: Localisation Barriers to Trade*, OECD Trade Policy Papers, No. 180 (Paris: OECD Publishing, 2011), http://dx.doi.org/10.1787/5js1m6v5qd5j-enOECD report on LCR **DEAD LINK**. According to the same OECD study, U.S. exports of digitally-enabled services grew from $282 billion in 2007 to $356 billion in 2011.

77 Cameron Kerry, "Missed Connections: Talking With Europe About Data, Privacy, and Surveillance," Brookings Center for Technology Innovation, May 2014, http://www.brookings.edu/~/media/research/files/papers/2014/05/20-europe-privacy-surveillance-kerry/kerry_europefreetradeprivacy.pdf.

78 In 2012, the European Commission proposed a set of ambitious new rules to amend its 1995 Data Protection Directive. But the provisions of the draft General Data Protection Regulation, which aims to strengthen the regime for data privacy and confidentiality in the general sense, have the potential to severely curtail cross-border data transfers to third countries that under the 1995 directive were able to outsource private data.

79 Martin A. Weiss and Kristin Archick, "The EU-U.S. Safe Harbor Agreement on Personal Data Privacy: In Brief," Congressional Research Service Report R44257, October 29, 2015, https://www.fas.org/sgp/crs/misc/R44257.pdf.

80 European Data Protection Supervisor, 2014.

81 European Court of Justice, "Judgment of the Court in Case C-362/14," October 6, 2015, http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=439476.

82 Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, and Bert Verschelde, "The Costs of Data Localization: Friendly Fire on Economic Recovery," ECIPE Occasional Paper No. 3/2014, European Center for International Political Economy, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

83 Hosuk Lee-Makiyama. "Data Localisation Requirement in Russia: A Self-Imposed Sanction," European Center for International Political Economy, June 10, 2015, http://www.ecipe.org/blog/data-localisation-russia/#.VXsXaqPu8H8.twitter.

84 Vicky Nanjappa, "Private Mail in Government Office: India Finally Acts," *OneIndia*, March 3, 2015, http://www.oneindia.com/feature/private-mail-in-government-office-india-finally-acts-1672212.html.

85 On September 9, 2013, the OECD published revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updating the original 1980 guidelines: "OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," July 11, 2013, http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

86 Article 28 of the framework states that "as part of establishing or reviewing their privacy protections, Member Economies, consistent with the APEC Privacy Framework and any existing domestic privacy protections, should take all reasonable and appropriate steps to identify and remove unnecessary barriers to information flows and avoid the creation of any such barriers." *APEC Privacy Framework* (Singapore: APEC Secretariat, 2005), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

87 "KORUS FTA Text," U.S. Korea Connect, accessed December 12, 2015, http://www.uskoreaconnect.org/about/korus/electronic-commerce.html.

88 Office of the United States Trade Representative, "TPP Full Text," https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text.

89 "B20 Trade Taskforce Policy Paper," September 2015, http://b20turkey.org/policy-papers/b20turkey_trade.pdf.

90 European Data Protection Supervisor, 2014.

91 "The Trade in Services Agreement (TiSA)," Coalition of Services Industries, accessed December 12, 2015, https://servicescoalition.org/negotiations/trade-in-services-agreement.

92 COM(2013) 847 final, "Communication From the Commission to the European Parliament and the Council on 'the Functioning of the Safe Harbour From the Perspective of EU Citizens and Companies Established in the EU,'" http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013DC0847.

93 European Data Protection Supervisor, 2014.

94 Kerry, "Missed Connections."

95 In its report on TTIP, the French Digital Council underlines the difficulty of distinguishing between personal data and commercial data: "What could be considered commercial data at first, such as information about a household's energy consumption, may provide information about the private life of the household (how many people live in the household, their personal activities, etc.) if the data are recorded and analysed minute by minute, or even second by second." In "Strengthening EU's Negotiation Strategy to Make TTIP a Sustainable Blueprint for the Digital Economy and Society," Conseil National du Numerique, April 2014, http://www.cnnumerique.fr/wp-content/uploads/2014/05/Version-web-ANGLAIS-19.05.pdf.

96 The EU Data Protection Working Party and the APEC Data Privacy Subgroup have already held meetings with a view to evaluating the interoperability of the EU's binding corporate rules and APEC's Cross-Border Privacy Rules.

97 This arrangement has its roots in the creation of the Internet, and before it Arpanet, which was established between four U.S. universities in 1969.

98 Patryk Pawlak, "Cyber World: Site Under Construction," EUISS Issue Brief No. 32, European Union Institute for Security Studies, September 2013, http://www.iss.europa.eu/uploads/media/Brief_32.pdf.

99 Tim Maurer and Robert Morgus, "Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate," Internet Governance Paper No. 7, Center for International Governance Innovation, May 5 2014, https://www.cigionline.org/publications/tipping-scale-analysis-of-global-swing-states-internet-governance-debate.

100 Ian Wallace, "India, the U.S., and Internet Governance," India-U.S. Policy Memo, Brookings Institution, September 2014, http://www.brookings.edu/research/opinions/2014/09/23-india-us-internet-governance-wallace.
101 George Christou and Seamus Simpson, "The Internet and Public-Private Governance in the European Union," *Journal of Public Policy* 26, no. 1 (January–April 2006): 43–61.
102 Thomas Renard, "The Rise of Cyber-Diplomacy: The EU, Its Strategic Partners and Cyber-Security," ESPO Working Paper No 7, European Strategic Partnership Observatory, June 2014, http://www.egmontinstitute.be/wp-content/uploads/2014/06/ESPO-WP7.pdf.
103 European Commission, 'Commission to Pursue Role as Honest Broker in Future Global Negotiations on Internet Governance," press release, February 12, 2014, http://europa.eu/rapid/press-release_IP-14-142_en.htm.
104 Brenden Kuerbis, "Reading Tea Leaves: China Statement on Internet Policy," Internet Governance Project, June 8, 2010, accessed December 12, 2015, http://www.internetgovernance.org/2010/06/08/reading-tea-leaves-china-statement-on-internet-policy/.
105 Rebecca MacKinnon, "The United Nations and the Internet: It's Complicated," *Foreign Policy*, August 8, 2012, http://foreignpolicy.com/2012/08/08/the-united-nations-and-the-internet-its-complicated/.
106 For instance, India refused to support the Statement of Principles agreed to at the NETMundial Global Multistakeholder Meeting on the Future of Internet Governance in Sao Paulo in April 2014.
107 "Indian Government Declares Support for Multistakeholder Model of Internet Governance at ICANN53," press release, Internet Corporation for Assigned Names and Numbers, June 22, 2015, https://www.icann.org/resources/press-material/release-2015-06-22-en.
108 Wallace, "India, the U.S., and Internet Governance."
109 "Basic Information: About WSIS," World Summit on the Information Society, United Nations International Telecommunication Union, accessed December 14, 2015, http://www.itu.int/wsis/basic/about.html.
110 World Summit on the Information Society WSIS-05/TUNIS/DOC/6(Rev. 1)-E, "Tunis Agenda for the Information Society," United Nations International Telecommunication Union, November 18, 2005, http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.
111 Larry Downes, "Why Internet Governance Should Be Left to the Engineers," *Washington Post*, September 3, 2014, http://www.washingtonpost.com/blogs/innovations/wp/2014/09/03/why-internet-governance-should-be-left-to-the-engineers/.
112 Jeremy Malcolm, "Internet Governance and the NETmundial Initiative: A Flawed Attempt at Turning Words Into Action," Electronic Frontier Foundation, August 28, 2014, https://www.eff.org/deeplinks/2014/08/internet-governance-and-netmundial-initiative-flawed-attempt-turning-words-action.
113 Anupam Chander, "Challenges and Approaches to Effective Cyberspace Governance in a Multipolar World," *Proceedings of the Annual Meeting (American Society of International Law)* 107 (April 2013): 95–110.
114 "New Treaty Signed but Not by All," Reporters Without Borders, December 21, 2012, http://en.rsf.org/internet-s-future-at-stake-at-itu-10-12-2012,43776.html.
115 A detailed breakdown of country positions can be found in Maurer and Morgus, "Tipping the Scale."
116 ITU News, "Member States React to New Treaty," Press Release, December 14, 2012, https://itunews.itu.int/en/3335-Member-States-react-to-new-treaty.note.aspx.
117 Jasmin Melvin, "Lawmakers Blast U.N. 'Power Grab' for the Net," Reuters, May 31, 2012, http://uk.reuters.com/article/us-internet-governance-congress-idUKBRE84T1EC20120531.
118 IANA is the department of ICANN responsible for the global coordination of the Domain Name Server root zone, Internet protocol (IP) addressing, and other Internet protocol resources.
119 Samuel Gibbs, "ICANN Chief: Shift Away From US 'is the Way Forward,'" *Guardian*, November 21, 2013, http://www.theguardian.com/technology/2013/nov/21/icann-internet-governance-solution-us-nsa-brazil-argentina.

120 Negroponte, Palmisano, and Segal, *Defending an Open, Global, Secure, and Resilient Internet*.
121 MacKinnon, "The United Nations and the Internet."
122 Carl Bildt, "The Future Global Order," Digital Power Series Part 1, European Council on Foreign Relations, July 20, 2015, http://www.ecfr.eu/article/commentary_the_future_global_order3072.
123 Office of Tax Policy, U.S. Treasury Department, "Selected Tax Policy Implications of Global Electronic Commerce," November 1996, https://www.treasury.gov/resource-center/tax-policy/Documents/internet.pdf.
124 Vanessa Houlder, "Internet Groups Face Global Tax Crackdown," *Financial Times*, March 24, 2014, http://www.ft.com/cms/s/0/e46350f6-b37d-11e3-bc21-00144feabdc0.html#axzz3WnjJaX6A.
125 Ibid.
126 Richard Rubin, "U.S. Companies Are Stashing $2.1 Trillion Overseas to Avoid Taxes," *Bloomberg Business*, March 4, 2015, http://www.bloomberg.com/news/articles/2015-03-04/u-s-companies-are-stashing-2-1-trillion-overseas-to-avoid-taxes.
127 Vanessa Houlder, "Special Tax Rules for Internet Companies 'Not Viable,'" *Financial Times*, January 20, 2014, http://www.ft.com/cms/s/0/ec659cec-81ef-11e3-a600-00144feab7de.html#axzz3Wj6HdkBw.
128 Frances Robinson and Sam Schechner, "France Pushes EU to Regulate U.S. Internet Companies," *Wall Street Journal*, September 19, 2013, http://online.wsj.com/news/articles/SB10001424127887324492604579085222987377040.
129 Eliza Anyangwe, "Addis Ababa Talks Risk Deadlock Over UN Agency for Tax," *Guardian*, July 15, 2015, http://www.theguardian.com/global-development-professionals-network/2015/jul/15/addis-ababa-talks-risk-deadlock-over-un-agency-for-tax-ffd3-financing-for-development.
130 United Nations Conference on Trade and Development, "Chapter 5: International Tax and Investment Policy Coherence," in *World Investment Report 2015: Reforming International Investment Governance* (Geneva: United Nations Conference on Trade and Development, 2015), http://unctad.org/en/PublicationChapters/wir2015ch5_en.pdf.
131 Organisation for Economic Co-operation and Development, *Action Plan on Base Erosion and Profit Sharing* (Paris: OECD Publishing, July 2013), http://www.oecd.org/ctp/BEPSActionPlan.pdf.
132 Jeremy Scott, "Can the United States Kill BEPS?" *Forbes*, June 16, 2015, http://www.forbes.com/sites/taxanalysts/2015/06/16/can-the-united-states-kill-beps/.
133 Martin O'Malley, "The U.S. Government – and the Next President – Needs to Take Cybersecurity Seriously," *Foreign Policy*, June 9, 2015, http://foreignpolicy.com/2015/06/09/the-u-s-government-and-the-next-president-needs-to-take-cybersecurity-seriously/.
134 James Lewis and Stewart Baker, "The Economic Impact of Cybercrime and Cyber Espionage," McAfee and the Center for Strategic and International Studies, July 2013, http://www.mcafee.com/tr/resources/reports/rp-economic-impact-cybercrime.pdf.
135 Toby Sterling and Thomas Escritt, "Dutch Government Website Outage Caused by Cyber Attack," Reuters, February 11, 2015, http://www.reuters.com/article/2015/02/11/us-netherlands-government-websites-idUSKBN0LF0N320150211.
136 Robert Wright and Andy Sharman, "Cyber Hack Triggers Mass Fiat Chrysler Car Recall," *Financial Times*, July 24, 2015, http://www.ft.com/intl/cms/s/0/2bafe3e0-321f-11e5-8873-775ba7c2ea3d.htmlv.
137 Andrea Shalal and Alina Selyukh, "Obama Seeks $14 Billion to Boost U.S. Cybersecurity Defenses," Reuters, February 2, 2015, http://www.reuters.com/article/2015/02/02/us-usa-budget-cybersecurity-idUSKBN0L61WQ20150202.
138 Kristin Finklea et al., "Cyber Intrusion Into U.S. Office of Personnel Management: In Brief," Congressional Research Service Report R44111, July 17, 2015, http://www.fas.org/sgp/crs/natsec/R44111.pdf.

139 Robert Rampton and Lisa Lambert, "Obama Warns China on Cyber Spying Ahead of Xi Visit," Reuters, September 16, 2015, http://www.reuters.com/article/2015/09/16/us-obama-roundtable-cybersecurity-idUSKCN0RG2AS20150916.

140 High Representative of the European Commission for Foreign Affairs and Security Policy, "Cybersecurity Strategy of the European Union."

141 Nicole Perlroth, "Online Security Experts Link More Breaches to Russian Government," *New York Times*, October 28, 2014, http://www.nytimes.com/2014/10/29/technology/russian-government-linked-to-more-cybersecurity-breaches.html.

142 Nicole Perlroth, "Russian Hackers Targeting Oil and Gas Companies," *New York Times*, June 30, 2014, http://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html.

143 Jordan Robertson and Michael Riley, "Mysterious 08' Turkey Pipeline Blast Opened New Cyberwar," *Bloomberg Business*, December 10, 2014, http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

144 David E. Sanger and Nicole Perlroth, "NSA Breached Chinese Servers Seen as Security Threat," *New York Times*, March 22, 2015, http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

145 Unit 61398 is just one of more than 20 cyberattack groups with origins in China, according to Mandiant. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria: Mandiant, 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

146 David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *New York Times*, February 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html.

147 Mandiant, *APT1*.

148 Ibid.

149 Bill Gertz, "NSA Details Chinese Cyber Theft of F-35, Military Secrets," *Free Beacon*, January 22, 2015, http://freebeacon.com/national-security/nsa-details-chinese-cyber-theft-of-f-35-military-secrets/.

150 Li Zhong, "New Law Better Safeguards National Security," *China Daily*, July 3, 2015, http://www.chinadaily.com.cn/opinion/2015-07/03/content_21169517.htm.

151 Wang Qun, "Statement by H. E. Mr. Wang Qun, Ambassador for Disarmament Affair of China, at the General Debate of the First Committee of the 66th session of UNGA," press release, Ministry of Foreign Affairs of the People's Republic of China, October 8, 2011, http://www.fmprc.gov.cn/eng/wjb/zzjg/jks/jkxw/t865572.shtml. **DEAD LINK.**

152 United Nations General Assembly, A/66/359, "Letter Dated 14 September 2011 From the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General," September 14, 2011, https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

153 Ellen Nakashima and Steven Mufson, "U.S., China Vow Not to Engage in Economic Cyberespionage," *Washington Post*, September 25, 2015, https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html.

154 Barack Obama, "Remarks by the President to the Business Roundtable," press release, White House, September 16, 2015, https://www.whitehouse.gov/the-press-office/2015/09/16/remarks-president-business-roundtable.

155 Rowena Mason, "Xi Jinping State Visit: UK and China Sign Cybersecurity Pact," *Guardian*, October 21, 2015, http://www.theguardian.com/politics/2015/oct/21/uk-china-cybersecurity-pact-xi-jinping-david-cameron.

156 The penultimate paragraph of the summit declaration reads: "We are living in an age of Internet economy that brings both opportunities and challenges to global growth. We acknowledge that threats to the security of and in the use of ICTs, risk undermining our collective ability to use the Internet to bolster economic growth and development around the world. We commit ourselves to bridge the digital divide. In the ICT environment, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations. In support of that objective, we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications. We also note the key role played by the United Nations in developing norms and in this context we welcome the 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs in accordance with UN resolution A/C.1/70/L.45. We are committed to help ensure an environment in which all actors are able to enjoy the benefits of secure use of ICTs." "G20 Leaders' Communique," http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/.

157 Joseph Nye, "International Norms in Cybersace," Project Syndicate, May 11, 2015, http://www.project-syndicate.org/commentary/international-norms-cyberspace-by-joseph-s--nye-2015-05#dyVf7iLKcYhSybZm.99.

158 Kennette Benedict, "Stuxnet and the Bomb," *Bulletin of the Atomic Scientists*, June 15, 2012, http://thebulletin.org/stuxnet-and-bomb.

159 United Nations General Assembly, A/65/154, "Developments in the Field of Information and Telecommunications in the Context of International Security," July 20, 2010, http://www.un.org/ga/search/view_doc.asp?symbol=A/65/154.

160 Executive Office of the President, *National Security Strategy* (Washington: White House, February 2015), https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

161 Office of the Secretary of Defense, *The Department of Defense Cyber Strategy* (Washington: U.S. Department of Defense, April 2015), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

162 Vladimir Platov, "Iran and Modern Cyber Warfare," Global Research, December 24, 2014, http://www.globalresearch.ca/iran-and-modern-cyber-warfare/5421360.

163 For an insightful account, see Kim Zetter, *Countdown to Zero Day. Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown Publishers, 2014).

164 Guilbert Gates, "How a Secret Cyberwar Program Worked," *New York Times*, June 1, 2012, http://www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html.

165 David E. Sanger, "US Decides to Retaliate Against China's Hacking," *New York Times*, July 31, 2015, http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html.

166 Brian Bennett, "Cyberattacks Pose Growing Threat to U.S., Intelligence Chief Says," *Los Angeles Times*, February 26, 2015, http://www.latimes.com/nation/la-na-intel-cyber-20150226-story.html.

167 Office of the Secretary of Defense, *The Department of Defense Cyber Strategy*.

168 Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor* 42 (October 7, 2013), http://carnegieendowment.org/files/CLM42MS.pdf.

169 PRC Information Office of the State Council, "China's National Defense in 2010," March 2011, http://www.fmprc.gov.cn/eng/wjb/zzjg/jks/kjfywj/t812036.shtml.

170 United Nations General Assembly, Resolution No. 68/167, "Developments in the Field of Information and Telecommunications in the Context of International Security," December 27, 2013, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/243.

171 United Nations Office for Disarmament Affairs, A/RES/53/70, "Developments in the Field of Information and Telecommunications in the Context of International Security," January 4, 1999, http://www.un.org/disarmament/topics/informationsecurity/.

172 United Nations General Assembly, A/70/174, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

173 United Nations General Assembly, A/66/359, "Letter Dated 12 September 2011 From the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General," September 14, 2011, https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.

174 Hamadoun I. Touré, "Cybersecurity Global Status Update," International Telecommunication Union, December 2011, http://www.un.org/en/ecosoc/cybersecurity/itu_sg_20111209_nonotes.pdf.

175 Organization for Security and Co-operation in Europe Permanent Council, Decision No. 1106, "Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming F rom the Use of Information and Communication Technologies," December 3, 2013, http://www.osce.org/pc/109168?download=true.

176 Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013), https://ccdcoe.org/tallinn-manual.html.

177 Benjamin Brake, "Cyberspace's Other Attribution Problem," *Net Politics* (blog), Council on Foreign Relations, August 5, 2015, http://blogs.cfr.org/cyber/2015/08/05/cyberspaces-other-attribution-problem/?cid=soc-twitter-cyberspaces_other_attribution_problem-80515.

178 Experts like Kennette Benedict are highly critical of the current U.S. stance, arguing that the "United States has much to lose from unrestrained cyberattack capabilities that might be spread around the world." See Benedict, "Stuxnet and the Bomb."

179 Richard J. Danzig, *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies* (Washington: Center for a New American Security, July 2014), http://www.cnas.org/sites/default/files/publications-pdf/CNAS_PoisonedFruit_Danzig_0.pdf.

180 Zetter, *Countdown to Zero Day*.

181 Michael Spehr, "Angriff auf IT-Systeme: Das Spiel der Hacker," *Frankfurter Allgemeine*, May 11, 2011, http://www.faz.net/aktuell/technik-motor/computer-internet/angriff-auf-it-systeme-das-spiel-der-hacker-1639819.html.

182 The Wassenaar Arrangement, an international code of conduct for regulating the export of dual-use technologies, was amended in December 2013 to include surveillance software.

183 Richard A. Clarke et al., *Liberty and Security in a Changing World*, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, December 12, 2013, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

184 James A. Lewis, "The Role of Offensive Cyber Operations in NATO's Collective Defence," Tallinn Paper No. 8, NATO Cooperative Cyber Defence Centre of Excellence, 2015, https://ccdcoe.org/multimedia/role-offensive-cyber-operations-natos-collective-defence.html.

185 Ibid.

CARNEGIE EUROPE

Founded in 2007, **Carnegie Europe** is the European center of the Carnegie Endowment for International Peace. From its newly expanded presence in Brussels, Carnegie Europe combines the work of its research platform with the fresh perspectives of Carnegie's centers in Washington, Moscow, Beijing, and Beirut, bringing a unique global vision to the European policy community. Through publications, articles, seminars, and private consultations, Carnegie Europe aims to foster new thinking on the daunting international challenges shaping Europe's role in the world.

The **Carnegie Endowment for International Peace** is a unique global network of policy research centers in Russia, China, Europe, the Middle East, and the United States. Our mission, dating back more than a century, is to advance the cause of peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

BEIJING BEIRUT BRUSSELS MOSCOW WASHINGTON

THE GLOBAL THINK TANK

CARNEGIE EUROPE

CarnegieEurope.eu