KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

UNPACKING "CYBERSECURITY": THREATS, RESPONSES, AND HUMAN RIGHTS CONSIDERATIONS

June 26, 2013

Public and private sector actors face a growing challenge in protecting the Internet and other ICT systems against malicious actors. Because ICTs are central to economic activity, human interaction, and democratic participation, cybersecurity policy can affect privacy, free expression, innovation, and the open flow of information. In order to develop effective responses to cybersecurity challenges and protect human rights, it is important first to understand that "cybersecurity" is an umbrella concept that covers a diverse range of threats and possible responses. Without unpacking the issue, policymakers are likely to develop overbroad policies that are not protective of – and that may be harmful to – human rights. Conversely, a clear vocabulary of cybersecurity threats and responses enables targeted, effective, and rights-respecting policies. This paper provides a starting point for such an approach by clarifying the range of issues often covered under the umbrella of cybersecurity and discussing the responses that may be put in place.

I. Introduction

Information and communications technologies (ICTs) are an increasingly important part of social, economic, and governmental activity around the world. At the same time, public and private sector actors face a growing challenge in protecting the Internet and other ICT systems against malicious actors. Attacks are becoming more sophisticated. Threats frequently cross state boundaries. In response, governments are considering what they can do to improve the security of their own and private sector systems.

However, precisely because ICTs are central to economic activity, human interaction, and democratic participation, cybersecurity policy can affect privacy, free expression, innovation, and the open flow of information. Some governments appear to be using cybersecurity as a pretext for establishing sweeping authority to silence controversial voices online or to conduct surveillance of citizens. In China, for example, the 2012 "Decision to Strengthen the Protection of Online Information" requires phone and Internet service providers to collect personal information about account holders, including real name identities of users who produce online content under pseudonyms.[1] A federal decree on cybercrime in the United Arab Emirates, also passed in 2012, includes vague provisions allowing authorities to prosecute citizens who criticize government policies or officials online.[2] As a growing number of countries are passing laws on computer crimes and security, even well-intentioned measures could have negative consequences, for example, by criminalizing common online behaviors in ways that give

[1] See Human Rights Watch, "China: Renewed Restrictions Send Online Chill" (January 4, 2013) http://www/hrw.org/news/2013/01/04/china-renewed-restrictions-send-online-chill.

[2] See Human Rights Watch, "UAE: Cybercrimes Decree Attacks Free Speech" (November 28, 2012) http://www.hrw.org/news/2012/11/28/uae-cybercrimes-decree-attacks-free-speech.

authorities broad discretion to prosecute or harass Internet users.[3]

For these reasons, policymakers and stakeholders must assess cybersecurity policies through a human rights lens (in addition to considering effectiveness and impact on innovation).

However, human rights activists should recognize that cybersecurity measures are not only a pretext for the suppression of speech or the invasion of privacy. To the contrary, a secure Internet is important for human rights, both of ordinary individuals and of human rights activists. It is well-documented that repressive regimes have targeted and infiltrated the computers of their political opponents and of human rights activists.[4]

In order to develop effective responses to cybersecurity challenges and protect human rights, it is important first to understand that "cybersecurity" is an umbrella concept that covers a diverse range of threats and possible responses. Until cybersecurity has been unpacked and specific solutions have been analyzed in relation to specific threats, policymakers are likely to develop overbroad policies that are not protective of – and that may be harmful to – human rights. Conversely, if there is a clear vocabulary of cybersecurity threats and responses, targeted and effective policies can be developed and rights-related abuses can be diminished.

This paper provides a starting point for such an approach by clarifying the range of issues often covered under the umbrella of cybersecurity. It is intended to help both civil society advocates and policymakers understand the complexity and diversity of threats and the appropriate range of responses, regulatory or otherwise, that may be put in place. This more nuanced understanding should assist in asking the right questions when discussing cybersecurity policy, in identifying what responses are appropriate for different aspects of the problem, and in choosing the appropriate forums (non-governmental, governmental, national, and international) through which to develop and implement such responses. It should yield solutions that are calibrated instead of overbroad. (For example, concerns about attacks on critical infrastructure have led to calls for a way to identify all Internet users in all contexts. However, a more calibrated approach would recognize that networks that manage power plants deserve strict identification requirements, but access to the Internet more generally should be permitted on an anonymous or pseudonymous basis in order to preserve key rights to seek, impart, and receive information.)

II. Assets, Attacks, Attackers, and Consequences

While there is no single agreed upon definition of cybersecurity, the European Union's cybersecurity strategy provides a helpful starting place for discussion:

> "Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security

[3] See Center for Democracy and Technology, "CDT Supports 'Aaron's Law' to Reform Federal Computer Crime Law" (June 20, 2013) https://www.cdt.org/pr_statement/cdt-supports-"aaron's-law"-reform-federal-computer-crime-law.

[4] See University of Toronto Munk Centre for International Studies, "Tracking Ghostnet: Investigating a Cyber Espionage Network" (March 29, 2009) http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network. See also Citizen Lab, "A Call to Harm: New Malware Attacks Target the Syrian Opposition" (June 21, 2013) https://citizenlab.org/2013/06/a-call-to-harm.

> strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."[5]

Importantly, this definition makes it clear that cybersecurity is limited to crimes against computers, not crimes that merely use computers. A wide range of crimes or civil offenses may be facilitated by computers (such as hate speech or defamation), but they should not be wrapped into the concept of cybersecurity. Computer crimes must be narrowly defined, so as not to cover common and legitimate behavior and so as not to be used to suppress speech or to control access to information. Instead, cybersecurity should focus on code-based or technology-based threats.

When evaluating cybersecurity policy proposals, it is important to define the assets that must be protected (the targets of attack or compromise); the specific type of attacks or exploits that the policy seeks to thwart; the nature of the attacker; and the consequences of a successful attack.[6] Specificity as to targets, methods, attackers, and consequences will support assessment of potential solutions.

A. Assets

The targets of cyberattack include information stored on computers or transmitted through computer networks:

- Personal data, including medical and financial data, stored on a personal computer or held in the database of a business;
- Confidential and sensitive email and other communications in real-time;
- Monetary funds, for example when attackers seek to transfer funds through account takeover or other means;
- Proprietary data, intellectual property, trade secrets and business plans;
- Non-public government data, including national security secrets.

Other times, the target is the computer or the network itself, as the attacker seeks to disrupt—

- The availability of an online service, such as an online banking service;
- Critical infrastructures (including energy, banking, transportation, and health care), which are increasingly dependent on computers and increasingly connected to the Internet;
- The availability of communications networks themselves, such as through attacks on the Domain Name System.

[5] "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," footnote 4, http://ec.europa.eu/information_society/newsroom/cf//document.cfm?doc_id=1667.

[6] There have been several comprehensive efforts to categorize cybersecurity. See Carol Myers, Sarah Powers, and Daniel Faissol, "Taxonomies of Cyber Adversaries and Attacks: a Survey of Incidents and Approaches" (April 2009) https://www-eng.llnl.gov/pdfs/taxonomies.pdf; James J. Cebula and Lisa R. Young, "A Taxonomy of Operational Cyber Security Risks," Carnegie Mellon CERT (2010) http://www.cert.org/archive/pdf/10tn028.pdf. The latter paper includes an appendix that specifically maps the numerous technical standards adopted by the U.S. National Institute of Standards and Technology against the proposed taxonomy of risks. For another effort to define key terms related to cybersecurity policy, see Russia-U.S. Bilateral on Cybersecurity, "Critical Terminology Foundations" (2011) http://www.ewi.info/cybersecurity-terminology-foundations. See also, Scott Charney, "Rethinking the Cyber Threat: A Framework and Path Forward" (2010) http://www.microsoft.com/en-us/download/details.aspx?id=747.

Increasingly, attackers conduct multi-stage attacks, taking over one computer or a series of computers in order to use them to launch an attack on the ultimate target.

B. Attacks

Attackers use a range of techniques to compromise computers, and they carry out attacks for a wide range of reasons:

- Gaining unauthorized access to a system by defeating a technical control to voyeuristically view private information without taking or destroying anything;
- Defacing a website or replacing existing content with images or slogans to make a political statement;
- Disrupting an online service, for example, by a denial of service attack that overwhelms the system so legitimate users cannot access it;
- Tricking a user (for example, through a "phishing email") into disclosing sensitive data, which is then used to compromise an account and steal or divert funds;
- Breaking into a computer (using various techniques) to gain control of its capabilities or information stored in it, which in turn may be used for theft of financial assets or for other purposes;
- Hijacking one computer to use it to attack other computers;
- Collecting intelligence (broadly defined) on an adversary (broadly defined);
- Theft of proprietary data or state secrets.

Cyberattacks may take place in conjunction with other crimes, such as the distribution of spam (unsolicited bulk messages). In the case of spam, attackers may hijack computers and use the machines to generate unwanted messages containing links or attachments that can compromise a recipient's computer.

C. Attackers

There is also a wide range of attackers, including:

- Teenagers breaking into the high school computer system;
- "Hactivists" seeking to make a political point;
- Criminals seeking to steal account credentials, personal information, or financial data;
- Terrorists;
- Nation states (or their affiliates) stealing proprietary data or national security secrets or spying on their adversaries (or their critics);
- Nation states (or their affiliates) planning or carrying out attacks to destroy or disrupt the physical or virtual assets of an adversary.

D. Consequences

Some attacks may be time-limited. For example, an e-commerce website may lose traffic and sales when it experiences a denial of service attack, but when the site is restored, the business can resume (having lost income, of course, and possibly suffering damage to its reputation).

Other assets once compromised may be difficult or impossible to recover. When sensitive health data is exposed, for example, the harm cannot be reversed. When the email accounts of human rights activists are hacked, they could face arrest, imprisonment, or death. When trade secrets are stolen, millions of dollars of research effort may end up benefiting a competitor. An attack on a control system might disrupt delivery of electrical power or other critical services and might even damage physical equipment. In an extreme case of armed conflict, cyberattacks on command, control, and communications systems may degrade a nation's ability to defend itself against physical attack.

III. Solutions

In response to this range of threats, governments, companies, and civil society use a diverse set of measures aimed at cyber threat prevention, response, and mitigation:

- hardware and software solutions;
- user education and training;
- Computer Security Incident Response Teams;
- voluntary design standards and best practices;
- corporate or governmental arrangements to share information about vulnerabilities and attacks;
- regulatory measures intended to mandate security improvements;
- the encouragement or imposition of measures for authentication or identification;
- criminal investigation and prosecution;
- national security responses (up to and including traditional military responses).

What is difficult but crucial is to identify the right targeted solution to any given aspect of the problem. It is clearly not desirable, for example, to turn the power of a nation's military on a teenage hacker breaking into a school computer. It is likewise disproportionate to impose identity requirements on all users for all purposes. It is also crucial to recognize that many solutions do not require the exercise of governmental power.

A. Non-Governmental Solutions

1. Product Design and Business Practices

Market forces are driving developers (of hardware, software, and applications) to improve the security of their products and services. On the web, for example, it is now becoming standard practice to use the HTTPS protocol (Hypertext Transfer Protocol Secure) to encrypt data in transit between a user's web browser and an online commerce site. Increasingly, companies are also encrypting data stored on laptops or in other portable media. Software companies produce a range of anti-virus and anti-malware tools for laptops, desktops, and servers and software companies offer regular security updates. Hardware companies build equipment with embedded security measures. Organizations may install firewalls to prevent malware from entering their networks and they may monitor traffic into and out of their networks and use various techniques to check for vulnerabilities on their systems.

In addition to technical solutions, businesses and organizations adopt best practices to protect systems and data. Best practices may be developed by industry groups, multistakeholder bodies, governments, or individual companies.

For example, the Messaging, Malware and Mobile Anti-Abuse Working (M3AAWG) brings together member companies in Asia, North America, and South America to collaboratively address messaging abuse issues, such as bots, spam, and DNS abuse. Among other activities, M3AAWG develops best practices for companies to improve online security and reduce messaging abuse (such as spam). The organization works closely with technical standards bodies, which sometimes leverage M3AAWG recommendations in their standards development work.[7]

In 2002, the Organisation for Economic Co-operation and Development (OECD) produced "Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security." According to the OECD, the guidelines are the "first international set of fundamental principles focused on the development of security policies in an open environment."[8]

Governments should recognize the value of best practices, and might seek to encourage their development, but governments should not seek to mandate product design or corporate practices. Because cyberattacks are so diverse and because they are constantly evolving, it is especially difficult for government to mandate specific security practices by individuals and businesses.

2. *Technical Standards*

Technical standards – essentially guidelines on how to build and operate software, devices, and systems – play an important role in security. Many standards bodies are non-governmental, global in nature, and open to all participants, making decisions based on consensus. This multi-stakeholder, voluntary process has proven remarkably effective.[9]

Standards bodies develop solution-based responses to many categories of cyber threats, addressed to many of the layers of the Internet's architecture. A leading example is the Internet Engineering Task Force (IETF), a non-governmental body that works on the basis of rough consensus. It is the leading developer of technologies to secure the Internet's core infrastructure. For example, the IETF maintains the standards used to secure the Domain Name System (DNS), the IP protocol, and web communications. It has working groups addressing a wide range of attack methods and tools to help improve operational security. The Managed Incident Lightweight Exchange (MILE) working group, for example, is building standardized data formats and communications mechanisms to help improve security incident information sharing.[10] Another group, focused on Network Endpoint Assessment (NEA), is developing standards for architectures that test whether an endpoint (the computer of an employee inside an organization) complies with the organization's policies for device security; by identifying devices that fail to meet security policies, organizations can take a range of steps to remediate the defect in the particular endpoint.[11] The World Wide Web Consortium (W3C), another multi-stakeholder standards body, has numerous security projects underway, including a Web Application Security Working Group.[12]

[7] See http://www.maawg.org.

[8] See http://www.oecd.org/sti/ieconomy/15582260.pdf.

[9] See Center for Democracy and Technology, "The Importance of Voluntary Technical Standards for the Internet and Its Users" (August 29, 2012) https://www.cdt.org/files/pdfs/Importance%20of%20Voluntary%20Technical%20Standards.pdf; Steve Mills, International Standards in the Emerging Global Economy, http://open-stand.org/wp-content/uploads/2012/11/International-Standards-in-the-Emerging-Global-Economy-V2.pdf.

[10] See http://datatracker.ietf.org/wg/mile/charter/.

[11] See http://datatracker.ietf.org/wg/nea/charter/.

[12] See http://www.w3.org/2011/webappsec/.

- **Human Rights Considerations:** There is a risk that standards can be manipulated to serve corporate or governmental interests in ways that are inimical to the open Internet. For example, governments have sought to require that surveillance capabilities be built into standards. In addition, some governments seek to require country-specific standards, which risk the fragmentation of the Internet. Global, multi-stakeholder standards bodies offer the best opportunity for those with expertise in protecting privacy or free speech to build human rights safeguards directly into technical standards. However, civil society advocates generally lack the resources to participate in those bodies. The IETF and the W3C have both made institutional commitments to ensuring that the standards they develop are privacy-protective and secure.

3. *Education*

Many cybersecurity incidents arise because legitimate users engage in unsafe practices by failing to update their software, clicking on unexpected attachments, or succumbing to malicious spam. As a result, their computers may become infected with viruses or taken over by others for nefarious purposes.

In response, companies and government agencies may seek to educate their employees on sound practices. Likewise, service providers, civil society groups, and government agencies may seek to educate consumers about individual security "hygiene."

For example, a growing number of Tibetan activists and citizens have been targeted by malware that shares a mobile phone user's device location, SMS message history, calls, and contacts with the attacker.[13] In response, the Tibetan Action Institute develops public education campaigns aimed at improving personal security practices and protecting human rights. The organization produces videos and flyers informing users about the different types of attacks and methods for preventing them, such as avoiding email attachments from unfamiliar senders.[14]

In addition, there are broader cyber-hygiene efforts, like those offered by http://www.staysafeonline.org. There are also company initiatives such as the botnet notification program at Comcast and best practices such as those developed by the Online Trust Alliance.[15] Intergovernmental groups, such as the Asia-Pacific Economic Cooperation forum (APEC), also sponsor campaigns to promote public awareness about cybersecurity issues.[16]

4. *Information Sharing and Collaboration*

Information sharing and collaboration can assist network operators in improving cybersecurity. For example, Computer Security Incident Response Teams (CSIRTs) have been established around the globe and can be formed to help institutions and networks respond to attacks as they occur. CSIRTs are established to "recognize, analyze, and

[13] Global Voices Advocacy, "Netizen Report: Tibetan Internet Users Targeted With Malware" (April 9, 2013) http://advocacy.globalvoicesonline.org/2013/04/09/netizen-report-tibetan-internet-users-targeted-with-malware/.

[14] See https://tibetaction.net/detach-from-attachments/.

[15] See http://www.otalliance.org/news/releases/botnetnotice.html.

[16] See http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information/Security-and-Prosperity-Steering-Group/Cybersecurity-Awareness-2012.aspx.

respond" to computer incidents with the goal of limiting the harm that threats may cause.[17] CSIRTs may be ad-hoc or formal, and can be assembled to serve any set constituency, such as a company, a government, or a geographical region.

One example of the success of voluntary information sharing and collaboration was the Conficker Working Group. Conficker was a sophisticated botnet "worm." In 2008, it was released on the Internet and rapidly infected millions of government, business, and home computers in over 200 countries. Very quickly, major Internet companies, ISPs, domain name registries, independent technologists, academic researchers, representatives from ICANN, and others from around the world came together and formed the Conficker Working Group. Governments also participated, but governments neither convened nor led the effort. The group rapidly developed and implemented measures that successfully stopped the spread of the worm, and then disbanded once the threat was addressed.[18]

- **Human Rights Considerations:** Cybersecurity systems are becoming increasingly automated, capable of constantly monitoring networks and automatically sharing threat information, however broadly it is defined by the system. Cyberthreat information may include personally identifiable information ("PII"); at the very least, it often includes addressing or attribution information. There is a risk that a cybersecurity information sharing program could result in the disclosure of huge amounts of information revealing communications patterns and data flows. It would be particularly troubling if this data flowed to the government. Therefore, programs for the sharing of information about cyber threats and vulnerabilities must be carefully designed. Preference should be given to "peer-to-peer" sharing among private networks as opposed to creating governmental hubs or centers for cyber information. Safeguards must be included to minimize the collection and use of PII and to ensure that any information shared among companies or with the government is used only for cybersecurity purposes.[19]

Collaboration on threats and responses can occur also though international multi-stakeholder entities such as the Internet Governance Forum (IGF)[20] and World Summit on the Information Society (WSIS).[21] The ITU also has a role to play in building the capacity of countries to understand and respond to the cybersecurity challenge.[22] These fora provide opportunities for companies, governments, and members of civil society to discuss solutions and share knowledge and best practices.

[17] See http://www.cert.org/csirts/csirt_faq.html#1

[18] "The Conficker Working Group Lessons Learned Document" (June 2010, published January 2011) http://www.confickerworkinggroup.org/wiki/.

[19] Center for Democracy and Technology, "CDT Calls for Data Privacy Safeguards in the EU Cybersecurity Directive" (June 6, 2013) https://www.cdt.org/blogs/jens-henrik-jeppesen/0606cdt-calls-data-privacy-safeguards-eu-cybersecurity-directive.

[20] See http://www.intgovforum.org/cms.

[21] See http://www.itu.int/wsis/index.html.

[22] "Cybersecurity Information Exchange Techniques (CYBEX)" http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybex.aspx.

B. Governmental Solutions

1. Securing Governmental Systems

Governments must secure their own networks – the computers and networks owned and operated by the government itself. Governments can protect their own systems directly through the requirements they specify for the equipment and services they procure for governmental use, by setting and enforcing rules for government employees, and by monitoring traffic to and from government computers. (Government monitoring of private sector networks is quite a different matter.)

2. Securing Private Networks and Systems

Governments may seek to use regulatory mechanisms to promote the security of private sector networks and computer systems. However, given the pace of technological change, governmental bodies are not likely to be the source of effective technical solutions. To the contrary, government mandates can be counterproductive. Cybersecurity requires speed and agility: the cybercriminals are highly adaptive, and all those involved in defending networks need to be able to respond rapidly to changing threats. Government technology mandates are likely to be rapidly outdated and may be inconsistent with globally agreed-to standards. The private sector is likely to have greater technical expertise than government regulators, and government mandates imposed on the private sector could stifle the innovation needed to stay ahead of cyberthreats. Further, direct government involvement is securing private networks may open the door to government monitoring and other interventions that risk human rights.

There may be a greater case for government regulation of the cybersecurity of critical infrastructures, such as systems providing electric power generation and distribution. While critical infrastructure is often privately owned and operated, the entities operating these networks – banks, companies that generate and supply gas and electric power, airlines and other transportation companies – are often heavily regulated for non-cybersecurity safety and security, so it may be appropriate to include such cyber concerns in the regulatory structure.

3. Data Protection

A specific focus of regulation may be on the protection of personal data held by companies regarding their customers. In Europe, for example, the Data Protection Directive requires that all data controllers "must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing." The Directive recognizes, however, the difficulty of specifying how much security is appropriate: "Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."[23] In the U.S., the Federal Trade Commission has taken an incremental approach to defining what is an acceptable level of security for companies that collect and process data about consumers.

[23] Article 17**,** Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT. Efforts are underway to replace the directive with a regulation, but that too will include data security provisions.

4. *Criminal Law*

Most countries have adopted criminal laws addressing attacks on the security and integrity of computer systems, making it a crime to steal data from computers, to access computer systems without authorization (“hacking”), to intercept communications, and to destroy computer data or interfere with the availability of computer systems.

The Council of Europe’s 2002 Convention on Cybercrime provides a framework for addressing cybercrime.[24] It includes provisions defining the essential elements of cybercrime as well as procedural provisions outlining the authorities that governments might use to investigate and prosecute computer crimes and crimes using computers and the means by which they can cooperate in exchanging information about cybercrime. While the COE Convention on Cybercrime is not a perfect instrument – for example, it includes matters that are not properly defined as cybercrimes – the COE has developed deep expertise in this area.[25] The Convention is open to ratification not only by members of the COE but by all states.

- **Human Rights Considerations:** Computer crimes must be narrowly defined, so as not to cover common and legitimate behavior and so as not to be used to suppress speech or to control access to information. Sometimes discussions of cybersecurity become combined with discussions about various kinds of illegal or undesirable content: harassment, libel, hate speech, child pornography, or blasphemy. While these offenses may be committed using the Internet, they are not issues of computer security. There is little benefit to addressing these crimes in the context of “cyber” issues, as traditional laws will likely cover offenses committed online or could be easily modified to do so.

  The Cyber Crime Prevention Act of 2012, passed into law in the Philippines, is one example of a broad cybercrime law that raised concern among human rights advocates. The law addressed a wide range of crimes, from illegal access, data interference, and device misuse to computer fraud and content-related offenses such as cybersex, spam, child pornography, and libel.[26] The Supreme Court of the Philippines put an indefinite hold on the bill after receiving 15 petitions challenging the act on legal grounds. Opponents of the bill cited concerns that its libel provisions would chill speech on the Internet.[27]

5. *Government Surveillance & Access to Stored Data*

Cybersecurity debates often touch on questions of government surveillance and government access to data held by private-sector service providers, because the investigation of cybercrimes often requires either real-time monitoring of communications or access to stored data. However, government demands for investigative powers are often motivated by a range of concerns that reach beyond cybersecurity.

[24] See http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

[25] See resources compiled at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/aboutpoc_EN.asp.

[26] See http://www.gov.ph/2012/09/12/republic-act-no-10175/.

[27] See http://sc.judiciary.gov.ph/features/oral_arguments/cybercrime.

Some governments have adopted data retention mandates requiring that communications service providers retain certain data to support government surveillance. Such requirements are controversial because data retained by a service provider may, absent specific legal and procedural safeguards, be subject to access by the government to investigate any crime and may be accessed by intelligence agencies. In addition, the more data that companies are required to retain, and the longer the retention period, the greater the risk that personal information could be breached, leaked, or otherwise abused.[28]

- **Human Rights Considerations:** A nation should have clear procedures meeting international human rights standards for government access to communications and stored data when needed for the investigation of crimes and the protection of national security. Such procedures should limit government intrusions, to assure businesses and consumers that the government cannot unjustifiably monitor their communications or seize their data. Governments should not undertake broad monitoring of private sector networks for cybersecurity purposes. While the government may appropriately monitor its own networks, the private sector should be responsible for monitoring private sector networks.

  In his 2013 report, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, noted that the laws of many countries do not provide adequately strong limits on governmental surveillance. As a result of technological change, the surveillance capabilities of governments have left gaps in their privacy protections. The Special Rapporteur also raised concerns about overly broad national security exceptions: "The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulations by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability."[29]

6. National Security and the "Law of War"

While there is disagreement about the precise definition of cyber warfare, there is growing recognition that existing international principles governing armed conflict also apply to cyberattacks.[30] In this regard, the NATO Cooperative Cyber Defense Centre of Excellence recently issued the Tallinn Manual.[31] Written by an independent group of experts, the manual examines how international norms – both those defining when nations may resort to

[28] See Center for Democracy and Technology, "Data Retention Mandates: A Threat to Privacy, Free Expression, and Business Development" (Nov. 11, 2011) and other resources complied at https://www.cdt.org/grandchild/data-retention-mandates.

[29] Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" (April 17, 2013) http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[30] See David E. Graham, "Cyber Threats and the Law of War," Journal of national Security Law and Policy (2010) http://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf. In 2011, the U.S. government issued a document entitled *International Strategy for Cyberspace*, which noted that "[t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace." However, the document cautioned that the "unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them."

[31] Tallinn Manual on the International Law Applicable to Cyber Warfare (2013) http://www.ccdcoe.org/249.html.

force and those addressing the conduct of armed conflict (also known as humanitarian law) – apply in the context of cyberspace. While not an official document, the Manual is important in showing how existing frameworks apply to cybersecurity.

- **Human Rights Considerations:** While some aspects of cybersecurity clearly implicate national security interests, it is not necessary to militarize the elements of a nation's cybersecurity program that concern civilian government systems and private sector networks. In March of 2013, for example, the U.S. House of Representatives expressly voted to leave management of cybersecurity programs affecting civilian agencies and the private sector in the hands of a civilian agency, amending a key legislative proposal that could have allowed primacy over cybersecurity to migrate to a military agency.

7. Coordination Between National Governments

Multiple intergovernmental groups have undertaken efforts to support the coordination of cybersecurity efforts among member states, providing various resources for managing threats that cross national borders.[32]

- The Group of Eight (G8): The G8 Subgroup on High-Tech Crime has in the past worked to enhance governmental capabilities and promote cooperation in preventing, investigating, and prosecuting cyber crimes. The Subgroup developed the 24-7 High-Tech Crime Point-of-Contact Network to allow law enforcement officials to get in contact across borders regarding cybercrime investigations.

- Organization of American States (OAS): In 2004, the OAS adopted the Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity,[33] and the OAS conducts various activities aimed at improving the capabilities of Member States in cybersecurity.[34]

- Asia-Pacific Economic Cooperation (APEC): APEC's Telecommunication and Information Working Group's Security and Prosperity Steering Group engages in activities to strengthen incident response, develop security guidelines, and promote cooperation on cyber issues.[35]

- International Telecommunication Union (ITU): The ITU has undertaken a range of activities relating to cybersecurity, but concerns were raised in 2012 when proposals were offered to amend the ITU basic treaty to include references to cybersecurity.[36]

[32] See UN Office on Drugs and Crime, "Comprehensive Study on Cybercrime" (Draft February 2013) http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[33] See http://www.oas.org/cyber/documents/AG-RES.%202004%20Cyber%20Security%20Strategy%20%28complete%29.pdf.

[34] See http://www.oas.org/cyber/aboutus.asp. See also http://www.oas.org/en/sms/cyber/.

[35] See http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information/Security-and-Prosperity-Steering-Group.aspx.

[36] Center for Democracy and Technology, "Security Proposals to the ITU Could Create More Problems, Not Solutions" (Sept. 6, 2012) https://www.cdt.org/files/pdfs/Cybersecurity_ITU_WCIT_Proposals.pdf. In the end, the treaty was amended to include a general provision encouraging nations to cooperate in ensuring the security of international telecommunication networks.

8. Identity, Authentication, and Attribution

There is a constellation of issues around identity, authentication, and attribution representing some of the most challenging areas for both cybersecurity and human rights. It is undeniable that access controls based on identity are an important component of cybersecurity. However, some governments have adopted "one-size-fits-all" solutions that seem more aimed at controlling speech than solving real cybersecurity problems. Real names registration, for example, is often called a cybersecurity necessity when in fact it can be used for suppressing free expression. A better approach to identity online starts from the premise that different levels of identity are appropriate for different functions. For example, the level of identity and authentication necessary to access the computer-based control system of a power plant is different from that required for an individual to engage in online banking and that is different from the kind of authentication necessary to publish a blog or read a newspaper online.[37] International human rights norms recognize the value of pseudonymous speech.[38]

IV. The Process for Developing Cybersecurity Solutions

As a complex policy issue, cybersecurity requires solutions at various levels, both national and international, and by means both non-governmental and governmental. It requires different kinds of approaches, including improving the practices of the private sector, educating users, strengthening law enforcement cooperation across borders, and promoting security through technical standards.

In this context, for many aspects of the cybersecurity problem, the best structures for improvement are likely to be multi-stakeholder rather than government-dominated and voluntary rather than mandatory. Effective solutions are most likely to be developed with the participation of a variety of stakeholders, including ICT companies (communications service providers, hardware and software makers, e-commerce companies, and other online services); the critical infrastructures that depend on the Internet; technologists; law enforcement agencies; human rights advocates; and users. Processes based on the principles of openness, transparency, and participation are not only likely to produce better security policies but those policies are more likely to respect innovation and human rights.

About the Center for Democracy & Technology

The Center for Democracy & Technology is a non-profit public interest organization working to keep the Internet open, innovative, and free. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in communications technologies. CDT is

[37] See Scott Charney, "Establishing End to End Trust" (Section IV) (2008) http://www.brreg.no/porvoo13/documents/Establishing_End_to_End_Trust.pdf. See also Center for Democracy and Technology, "Privacy Principles for Identity in the Digital Age" (December 2007) https://www.cdt.org/files/pdfs/20071201_IDPrivacyPrinciples.pdf, and Center for Democracy and Technology, "Privacy and Identity Management" (2008) https://www.cdt.org/privacy/2008schwartzcooper.pdf.

[38] See Center for Democracy and Technology, "Regardless of Frontiers: The International Right to Freedom of Expression in the Digital Age" (Section IV E) (April 2011) https://www.cdt.org/files/pdfs/CDT-Regardless_of_Frontiers_v0.5.pdf.

dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

For further information, contact Matthew Shears, Director of CDT’s Project on Global Internet Policy and Human Rights, mshears@cdt.org, or Gregory T. Nojeim, Senior Counsel and Director of CDT's Project on Freedom, Security and Technology, gnojeim@cdt.org.