The Heritage Foundation

BACKGROUNDER

No. 3223 | JULY 14, 2017

Cybersecurity Beyond U.S. Borders: Engaging Allies and Deterring Aggressors in Cyberspace

David Inserra

Abstract

Cyberspace is a unique realm that challenges the U.S. in multiple ways. These challenges include the cyber domain's reach, speed, anonymous nature, and offense-dominated conflict. Given that cyberspace is an environment defined by ubiquity and anonymity and that cyberspace also has physical components and people located in different places around the world, international cybersecurity efforts are both important and difficult. Working together on cyber issues includes military cooperation with allies as well as working together to strengthen civilian cyber defenses to make hacking more difficult and less lucrative. Beyond cyber defense and offense, pushing and working with nations around the world to combat cybercrime and punish those who engage in aggressive cyber behavior themselves can help reduce the number of cyber attacks.

Cyberspace is a domain that has revolutionized the world. Massive amounts of data can be communicated from device to device from the other side of the room or the other side of the world. The number of services that are now available to the average consumer through a personal computer, smartphone, or other device are truly mindboggling. Banking, ride or apartment sharing, dissemination of information and media, video sharing and conferencing, social media, entertainment and gaming, buying and selling of goods, and countless other online activities are now second nature to most Americans, not to mention billions of individuals elsewhere.

With such leaps in productivity and convenience has come the opportunity for hackers and certain nation states to abuse this domain to steal, undermine, destroy, or manipulate these systems and masses of data for their own purposes. Since this domain is

Key Points

- It is time for the U.S. to build deeper ties and take greater action with nations that truly want to counter crime and economic espionage in cyberspace. The U.S. should strive to make existing cyber relationships more robust and meaningful.
- When faced with an offense-dominated domain and a particularly aggressive bad actor, the U.S. should raise the costs of hacking through various types of tailored retaliation. Such retaliation could include military, intelligence, diplomatic, legal, information, finance, and economic (MIDLIFE) tools.
- The U.S. needs a bolder strategy for how it will operate in the cyber domain. From deterring and retaliating against cyber aggressors to reinforcing cybercrime defense with allies, the U.S. should craft a new strategy that will direct the whole of government to protect U.S. interests in cyberspace.
- This strategy should also consider the central role of the private sector.

This paper, in its entirety, can be found at **http://report.heritage.org/bg3223**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

spread across the world, bad actors in cyberspace can accomplish their goals from thousands of miles away. As a result, when considering cybersecurity policies, the U.S. cannot just think about its own laws, resources, and systems but must also consider what is occurring outside its territory. Indeed, the U.S. must engage with its allies and partners to craft solutions that cross borders, while using traditional tools of national power to retaliate against nations that harbor or engage in malicious cyber activity. Only through such U.S. leadership will cyberspace continue to be a domain that is sufficiently secure to continue to promote prosperity and liberty.

The Nature of Cyberspace

Cyberspace is a unique realm that challenges the U.S in multiple ways. Specifically, these challenges include the cyber domain's reach, speed, anonymous nature, and offense-dominated conflict. Understanding the nature and challenges of this realm is important to understanding where and how the U.S. can take international action on cyber threats.

Cyberspace can be defined as "the manmade domain and information environment we create when we connect together all computers, wires, switches, routers, wireless devices, satellites, and other components that allow us to move large amounts of data at very fast speeds."[1] Cyberspace is distinguished by three unique features that not only support productive activities, but also can be used against the United States: Cyberspace is (1) ubiquitous, (2) anonymous, and (3) offense dominated.

1. Ubiquitous. Cyberspace is defined largely by its vast reach and the ability of an individual computer to communicate with any computer in the world.[2] There were an estimated 2.6 billion smartphone users in 2014, and an estimated total of 6.4 billion cyberspace-connected devices known as the "Internet of things."[3] Each of these devices has the ability to access information and send or receive commands across the Internet, interacting with any number of other devices. As the most technologically advanced military in the world, the U.S. military makes use of cyberspace in numerous ways, profoundly changing the way the military operates. In addition to U.S. military capabilities, the U.S. homeland depends on 16 sectors of interdependent critical infrastructure, most of which are reliant on cyberspace. The Department of Homeland Security, together with other government agencies, is responsible for protecting them. Beyond military and critical infrastructure systems, hundreds of millions of individuals in the U.S., not to mention billions across the world, take advantage of cyberspace for social, political, financial, and business reasons.

2. Anonymous. Perhaps the most-remarked feature of cyberspace is its anonymity. It is difficult to discern the exact origin of a cyberspace attack. First, an attack must be noticed, which is not always immediate. Then, forensic analysis of the attack mechanism must be undertaken to pinpoint the source of the intrusion. Depending on the complexity or type of attack, this process could take a significant amount of time, and, even if the geographic origin of the attack is confirmed, it may be difficult to determine who is responsible. This problem is exacerbated by the ability of hackers to redirect their attacks through other locations. Yet, for all the difficulty ascribed to attributing cyber attacks, the "attribution problem" may be overstated. The ability to break through the anonymity of cyber attacks and hacks is improving as evidenced by multiple notable private-sector attribution reports.[4] In some cases, a devastating cyber attack could be sourced by placing the attack in the context of other global affairs. Additionally, while any one hacking incident may be difficult to attribute, a series or campaign of hacks gives more data points with which to identify the attack-

[1] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, Vol. 73 (Second Quarter 2014), pp. 12–19.

[2] Robert Belk and Matthew Noyes, "On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy," Harvard KennedySchool Belfer Center, March 20, 2012, http://belfercenter.ksg.harvard.edu/publication/22046/on_the_use_of_offensive_cyber_capabilities.html (accessed May 16, 2017).

[3] Andy Boxell, "The Number of Smartphone Users in the World Is Expected to Reach a Giant 6.1 Billion by 2020," *Digital Trends*, June 3, 2015, http://www.digitaltrends.com/mobile/smartphone-users-number-6-1-billion-by-2020/ (accessed March 13, 2017), and Julia Boorstin, "An Internet of Things that Will Number Ten Billions," CNBC, February 1, 2016, http://www.cnbc.com/2016/02/01/an-internet-of-things-that-will-number-ten-billions.html (accessed March 13, 2017).

[4] Jim Finkle and Ron Grover, "Sony Hires Mandiant After Cyber Attack, FBI Starts Probe," Reuters, December 1, 2014, http://www.reuters.com/article/us-sony-cybersecurity-mandiant-idUSKCN0JE0YA20141201 (accessed March 10, 2017).

er. Still, the attribution challenge and anonymous nature of cyberspace do complicate U.S. responses to cyber incidents.

3. Offense-Dominated. For multiple reasons, cyberspace is currently considered an offense-dominated domain. It is easier, cheaper, and generally more effective to engage in offense than in defense. Cyber action, though, which sometimes takes months to prepare, takes place at the blink of an eye, and the types of attacks are constantly changing. There are also millions of potential targets vulnerable to exploitation. The attacker has to find just one hole to exploit, making cyber aggression an appealing and cheap form of asymmetric warfare. This attracts a whole range of bad actors, from cybercriminals looking to get rich quick to nation-states looking for top secret information or vulnerabilities in another nation's critical infrastructure or warfighting capabilities.[5]

U.S. International Efforts on Cybersecurity

Given that cyberspace is an environment defined by ubiquity, anonymity, and offense-dominance and that cyberspace also has physical components and people located in different places around the world, international efforts on cybersecurity are both important and difficult. They are important because passive or even active defense cannot always stop hackers, who see low-risk, high-reward opportunities everywhere. Working together on cyber issues includes military cooperation with allies as well as working together to strengthen civilian cyber defenses to make hacking more difficult and less lucrative.

Beyond cyber defense and offense, pushing and working with nations around the world to combat cybercrime and punish those who engage in aggressive cyber behavior themselves can help reduce the number of cyber attacks. Of course, relative anonymity and nations' geopolitical goals that run counter to U.S. interests make such efforts more difficult. Additionally, differing approaches to privacy can also pose a stumbling block to U.S. collaboration with other nations.

U.S. efforts on international cybersecurity were first and most notably articulated in the U.S.'s International Strategy for Cyberspace. Released in 2011, this strategy's express goal is to

> work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace.[6]

Such a goal is laudable, but the question is: How can the U.S. achieve this "open, interoperable, secure and reliable" cyberspace? The Obama Administration called for the development of norms that are based on freedom, privacy, property rights, the right to self-defense, and other principles.[7] While the principles are excellent, they are limited in effectiveness since other nations do not necessarily hold these same values. It is unlikely that China or Russia will agree to a set of norms that include key protections of individual privacy, freedom to access the full Internet, or respect for property rights. Even among allies, differences over norms such as privacy may complicate meaningful cooperation.

The limits of norm setting is best displayed by the Budapest Convention on Cybercrime. As "the only binding international instrument" on cybercrime, the convention seeks to help nations in the development and implementation of counter-cybercrime programs.[8] While this is a positive step in getting some countries to affirm their commitment to combatting cybercrime and promoting a free and secure Internet, arguably the largest sources of cyber threats, Russia and China, have not signed

[5] Bruce Schneier, "Understanding the Threats in Cyberspace," Schneier on Security, October 28, 2013, https://www.schneier.com/blog/archives/2013/10/understanding_t_2.html (accessed March 10, 2017).

[6] The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011, p. 8, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed March 10, 2017).

[7] Ibid., p. 9.

[8] Council of Europe, "Budapest Convention and Related Standards," http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (accessed March 10, 2017).

this convention.[9] Furthermore, even some of the nations that have adopted the convention are not committed to or capable of fully implementing these norms. Ukraine is a prime example of a nation that has adopted the Budapest Convention but is a known haven for cybercriminals.[10] Similarly, former Secretary of State John Kerry and National Security Agency head Admiral Michael Rogers advocated for international law for cyberspace.[11] More specifically, Rogers advocated an Internet subject to global rules similar to the U.N. Convention on the Law of the Sea (UNCLOS), which provides a clear example of the challenges of multinational treaties.[12]

While there are a myriad of potential problems with UNCLOS,13 the one most relevant to cybersecurity deals with how nations are supposed to settle disagreements through an arbitration panel. Quite tellingly, China has rejected the ruling of UNCLOS arbitration that the Philippines initiated against China over territorial claims in the South China Sea.[14] If China will not submit to a law to which it is a signatory in the physical world, there is no reason to believe that China, or other aggressive cyber nations, will comply with nebulous international law in cyberspace.

Thus, while norms may establish some baseline for some nations to agree on certain aspects of cybercrime, norms development is not enough. The International Strategy for Cybersecurity seems to recognize this, as it also mentions the need for dissuading and deterring enemies. Even the strategy, however, depends on the Budapest Convention and international law enforcement cooperation for combatting cybercrime.[15] Cyber deterrence must extend beyond just Budapest Convention signatories if it is to be truly effective at countering hackers.

For the past decade, the U.S. has generally preferred non-confrontational tactics, such as trying to cooperate with nations like China, despite their likely bad faith. General Martin Dempsey as Chairman of the Joint Chiefs of Staff and Hillary Clinton as Secretary of State both called for increased cooperation with China as the U.S. and China were, in the words of Secretary Clinton, both "victims of cyberattacks," drawing a moral equivalence between the robber and robbed.[16] However, after a long series of significant and publicized hacks by the Chinese government, the U.S. government came to recognize the need for more aggressive deterrent action against bad cyber actors. In 2013, the Obama Administration began to openly blame China for campaigns of cyber espionage directed at U.S. companies and government agencies, and in May 2014, it indicted five members of the Chinese People's Liberation Army on charges of cyber theft, the first time the U.S. has taken legal action against a foreign government for cybercrimes.[17]

[9] Council of Europe, "Chart of Signatures and Ratifications of Treaty 185," http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG (accessed March 10, 2017).

[10] Mark Clayton, "How Ukraine Crisis Could Dent Country's Booming Cyber-Crime," *The Christian Science Monitor*, March 26, 2014, http://www.csmonitor.com/World/Passcode/2014/0326/How-Ukraine-crisis-could-dent-country-s-booming-cyber-crime (accessed March 10, 2017), and Taylor Armerding, "Ukraine Seen as a Growing 'Haven' for Hackers," CSO, March 13, 2012, http://www.csoonline.com/article/2131155/network-security/ukraine-seen-as-a-growing--haven-for-hackers-.html (accessed March 10, 2017).

[11] Daniel Halper, "Kerry: Internet 'Needs Rules to Be Able to Flourish and Work Properly,'" *The Weekly Standard*, May 18, 2015, http://www.weeklystandard.com/blogs/kerry-internet-needs-rules-be-able-flourish-and-work-properly_949526.html# (accessed March 10, 2017).

[12] Eric Auchard and David Mardiste, "NSA Chief Urges 'Safe' Internet Under Equivalent of Law of the Sea," Reuters, May 27, 2015, http://www.reuters.com/article/2015/05/27/cybersecurity-nsa-idUSL5N0YI2KD20150527 (accessed March 10, 2017).

[13] Steven Groves, "Accession to the U.N. Convention on the Law of the Sea Is Unnecessary to Secure U.S. Navigational Rights and Freedoms," Heritage Foundation *Backgrounder* No. 2599, August 24, 2011, http://www.heritage.org/defense/report/accession-the-un-convention-the-law-the-sea-unnecessary-secure-us-navigational.

[14] Tom Phillips, Oliver Holmes, and Owen Bowcott, "Beijing Rejects Tribunal's Ruling in South China Sea Case," *The Guardian*, July 12, 2016, https://www.theguardian.com/world/2016/jul/12/philippines-wins-south-china-sea-case-against-china (accessed March 10, 2017).

[15] The White House, "International Strategy for Cyberspace," p. 20.

[16] Steven Bucci, "Secretary Clinton Declares U.S. and China Equal as Cyber Victims," The Daily Signal, September 6, 2012, http://dailysignal.com/2012/09/06/secretary-clinton-declares-u-s-and-china-equal-as-cyber-victims/, and David Inserra, "U.S. Should Stand Up to China on Cyber Attacks," The Daily Signal, May 1, 2013, http://dailysignal.com/2013/05/01/u-s-should-stand-up-to-china-on-cyber-attacks/.

[17] U.S. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014, http://www.justice.gov/opa/pr/2014/May/14-ag-528.html (accessed March 10, 2017).

Following the 2015 cyber breach of the Office of Personnel Management and at least 21.5 million personal records that included background investigations and security clearance data—believed to be the work of China—the Obama Administration laid the groundwork for firmer actions against malicious cyber actors. It promulgated Executive Order (EO) 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," which made clear the Administration's ability to sanction major hackers, their sponsors and supporters, and any beneficiaries of hacking who know the hacked material to be stolen.[18] Instead of using this authority against any number of Chinese activities, the U.S. and China came to an agreement to stop cyber economic espionage and work together to stop cybercrime. This agreement represents a return toward the Obama Administration's early policy of seeing both the U.S. and China as victims, misunderstanding China's interests and strategy.[19]

In the 2016 American election cycle, the Russian government undertook a series of hacks on U.S. election and political organizations, most notably the Democratic National Committee.20 The intelligence community identified the Russian government as the responsible party,[21] and the Obama Administration expelled a number of Russian diplomats and intelligence officials living in the U.S. The Administration also, for the first time, used EO 13694 to sanction four Russian individuals and five organizations.

While the Obama Administration did take some (uneven) steps to advance the U.S. international cybersecurity agenda, the overall policy of the U.S. was defined by hesitance to respond firmly to cyber aggression.

Policy Options for Combatting Cybercrime and Espionage

If the U.S. is to take a more active role in combatting cybercrime and espionage, a more comprehensive set of policies is needed from across all elements of national power. Conceptually, many experts use diplomacy, information, military, economics (DIME) and MIDLIFE (military, intelligence, diplomacy, legal, information, finance, economic) to refer to categories of tools available to policymakers.[22] In cyberspace, applying the all-tools-of-national-power approach means that the U.S. should consider the following policy areas as options for dealing with cyber aggression:

- Preparing for and defending against cyber aggression:
    - Improving global cooperation in combatting cybercrime, and
    - Greater collaboration with allies and partners on cybersecurity.
- Responding to cyber aggression:
    - Diplomatic responses,
    - Legal and economic responses, and
    - Strategic responses.

Preparing for and Defending Against Cyber Aggression

The U.S. is engaging with like-minded nations on cybersecurity through the Budapest Convention, NATO, and bilateral relations. The results of such relationships include the sharing of best practices

[18] U.S. Department of the Treasury, "Executive Order 13694: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," *Federal Register*, April 1, 2015, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf (accessed March 10, 2017).

[19] Dean Cheng, "Winning Without Fighting: The Chinese Psychological Warfare Challenge," Heritage Foundation *Backgrounder* No. 2821, July 12, 2013, http://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge.

[20] April Glaser, "Here's What We Know About Russia and the DNC Hack," *Wired*, July 27, 2016, https://www.wired.com/2016/07/heres-know-russia-dnc-hack/ (accessed March 10, 2017).

[21] News release, "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security," U.S. Department of Homeland Security, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national (accessed May 31, 2017).

[22] Paul Rosenzweig, "The Organization of the U.S. Government and Private Sector for Achieving Cyber Deterrence," Proceedings of a Workshop on Deterring Cyberattacks, National Research Council, 2010, https://www.nap.edu/read/12997/chapter/18 (accessed May 11, 2017).

Deterrence, Playing Hardball, or Something Else?

A significant question within the security research community is whether cyber deterrence is possible and where it should apply. Some experts view deterrence as a critical tool to develop while others view it positively but note that it may be difficult to establish or could have limited use. Still other experts view deterrence as a flawed or improper solution to the challenges the U.S. faces in cyberspace.*

Deterrence is the ability to dissuade an adversary from engaging in a certain kind of behavior due to the adversary's belief that the cost of that behavior would be untenable to him. There are two forms of deterrence—deterrence by denial and deterrence by punishment. Deterrence by denial relies on creating defenses that are strong enough to prevent an attack or minimize the impact of any attack that does take place. Thus, an adversary may be deterred if he believes an attack will fail or have only a minimal impact. Deterrence by punishment, on the other hand, promises serious consequences that are unacceptably costly to the attacker. So, a country could literally succeed in accomplishing its objectives but is deterred because it would be subject to counter attack of a level that it is unwilling or unable to endure.

Both forms of deterrence are discussed in the cybersecurity context. Due to the constantly changing and offense-dominated nature of cyberspace, defense and denial are difficult, especially in the face of a determined adversary, such as a nation-state actor. Still, improving cyber defenses may make cyber attacks, particularly from non-state actors, less successful and provide some level of deterrence. Deterrence by punishment seems, on its face, to be a far more effective solution for cyberspace, but it faces its own challenges. When struck by a cyber attack, the U.S. has a series of tools at its disposal ranging from cyber to diplomatic, that can punish an adversary. Attribution is one of the significant challenges to such deterrence, but it is increasingly clear that attribution is often possible if enough resources are applied. Another challenge in cyberspace is that, unlike nuclear weapons that are at the top of the escalation ladder, cyber incidents can be anything from a nuisance to a potentially existential threat, making an appropriate and proportional response more difficult.

There is of course a difference between destructive attacks on the U.S. and campaigns of economic espionage or information warfare. The vast majority of the literature on deterrence focuses on acts of war, often of the nuclear variety. Applying such concepts to lesser acts of aggression is not an exact fit, and this is perhaps the reason why some experts do not think deterrence is the correct answer for the cyber challenges the U.S. regularly faces. That said, making it more costly for adversaries to spy, steal, or attack the U.S. in cyberspace is something worth pursuing.

* James A. Lewis, "Deterrence in the Cyber Age," Center for Strategic and International Studies, November 13, 2014, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/141117_Lewis.pdf (accessed March 10, 2017); Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (accessed May 17, 2017); Dmitri Alperovitch, *Towards Establishment of Cyberspace Deterrence Strategy* (Tallin, Estonia: CCD COE Publications, 2011), p. 91, https://ccdcoe.org/ICCC/materials/proceedings/alperovich.pdf (accessed May 21, 2017); Adam Segal, "Sanctioning Hackers," Council on Foreign Relations, April 1, 2015, http://blogs.cfr.org/cyber/2015/04/01/sanctioning-hackers/ (accessed March 10, 2017); Dorothy Denning, "Cybersecurity's Next Phase: Cyber Deterrence," *Scientific American* (December 13, 2016), https://www.scientificamerican.com/article/cybersecuritys-next-phase-cyber-deterrence/ (accessed March 10, 2017); and Susan Hennessey, "Is US Cyber Deterrence Strategy More than (Russian) Roulette?" *Lawfare* (October 12, 2016), https://www.lawfareblog.com/us-cyber-deterrence-strategy-more-russian-roulette (accessed March 10, 2017).

to combat cybercrime, enabling information sharing on cyber threats and crimes, expanding and improving cybercrime legislation, enhanced law enforcement, and judicial cooperation including the extradition of cybercriminals, cybersecurity exercises, and military-to-military cooperation and training.[23] It is time for the U.S. to build deeper ties and take greater action with nations that truly want to counter crime and economic espionage in cyberspace. The U.S. should strive to make existing cyber relationships more robust and meaningful by committing to more cooperation and defensive cyber measures.

Improving Global Cooperation in Combatting Cybercrime. Given the international nature of cybercrime, combatting it requires international cooperation. As mentioned, the Budapest Convention on Cybercrime is the primary mechanism for nations to cooperate on cybercrime investigations. Unfortunately, expansion of the convention to additional countries has ground to a crawl, and key centers of cyber criminality, such as Russia and China, as well as Brazil and India, will not join the convention. Russia and China directly benefit from a great deal of the hacking that occurs and have no incentive to participate in the convention. India and Brazil refuse to join on principle, as the convention was originally developed by Europe and select other countries without their input.[24] While 52 nations have ratified the convention,[25] significantly more ratifications are unlikely.

Thus, the U.S. is seemingly left with two options—pushing for deeper cooperation with those who have ratified the convention or pursuing expansion of the convention. These two alternatives are not necessarily mutually exclusive, but given that the pace of accessions to the treaty has slowed down, the U.S. would be better served working to deepen the commitment and collaboration among those countries that are party to the convention now. This means taking tangible steps that expand how law enforcement organizations work together to fight cybercrime.

Expansion of active cyber defenses that identify hackers is an example of such cooperation. Many countries currently outlaw any unauthorized access to computers in their country. This means that certain types of active defenses are technically illegal even though they may greatly help identify hackers. One such active defense is a beacon that is attached to a company's files, similar to the way a LoJack tracker can be installed in cars, or dye packs attached to clothing or bags of money. When the files are stolen, a beacon is capable of reporting data back to the home network about where it is or who has stolen it. Such data would be extremely helpful to give to law enforcement but is likely illegal since the beacon accesses the hacker's computer without his authorization. Essentially, laws meant to outlaw hacking are actually protecting hackers from counter actions by responsible, law-abiding organizations. The U.S. should revise the way in which such active defense measures are viewed, both informally and statutorily with our allies. Allowing U.S. and German companies to locate, but not destroy, a hacker's computer, is in both the U.S. and Germany's interests and would truly deepen international cooperation in stopping cybercrime.

Another way the U.S. can deepen cooperation on combatting cybercrime with partner nations is to expand tools used in combatting transnational criminal organizations (TCO) to cybercrime organizations. While individual hackers and hacktivists certainly pose a problem, many sophisticated cybercriminals are part of larger criminal syndicates that often are spread across multiple different countries. In 2011,

[23] Council of Europe, "Budapest Convention and Related Standards"; Council of Europe, "Global Project on Cybercrime (Phase 3)," November 28, 2012, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_project_Phase3_2571/2571_Phase3_summary_V8_nov2012.pdf (accessed March 10, 2017); North Atlantic Treaty Organization, "Sharing Malware Information to Defeat Cyber Attacks," NATO, December 4, 2014, http://www.nato.int/cps/en/natolive/news_105485.htm?selectedLocale=en (accessed March 10, 2017); "Japan, U.S. Agree to Beef Up Cybersecurity," *The Japan Times*, October 3, 2013, http://www.japantimes.co.jp/news/2013/10/03/national/politics-diplomacy/japan-u-s-defense-chiefs-meet-on-cybersecurity/#.VAinmRa8GmE (accessed March 10, 2017); and news release, "Fact Sheet: U.S.–United Kingdom Cybersecurity Cooperation," U.S. Embassy & Consulates in the United Kingdom, January 16, 2015, https://uk.usembassy.gov/fact-sheet-u-s-united-kingdom-cybersecurity-cooperation/?_ga=1.231071391.1218445673.1489177409 (accessed March 10, 2017).

[24] CSIS Cyber Policy Task Force, "From Awareness to Action; A Cybersecurity Agenda for the 45th President," Center for Strategic and International Studies, January 2017, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf (accessed March 10, 2017).

[25] Council of Europe, "Chart of Signatures and Ratifications of Treaty 185," http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG (accessed March 10, 2017).

the Obama Administration released a "Strategy to Combat Transnational Organized Crime," including cybercrime as one of the areas that must be tackled. In part, this means having the domestic and international resources to investigate and find such organizations. It also means applying tools like the Racketeer Influenced and Corrupt Organizations (RICO) Act to cybercrime, and working with foreign governments to expand the use of RICO-equivalent laws against cyber criminals. In 2011, the Obama Administration requested that 18 U.S. Code § 1030—the Computer Fraud and Abuse Act—be added as one of the predicate offenses that can be used in a RICO case. Not only is RICO a useful tool in combatting criminal enterprises, it also opens guilty parties to further civil damages.[26]

Another idea, proposed by a bipartisan set of policymakers and experts at the Center for Strategic International Studies suggested punishing nations that refuse to cooperate in combatting cybercrime. They suggest that "penalties for the noncooperative could mirror the Financial Action Task Force (FATF) 'blacklist' of noncooperative countries,"[27] which applies to countries that are unable or refuse to help in combatting money laundering and terrorist financing efforts.[28] The signatories of the Budapest Convention could move to create a FATF-like organization that monitors the cooperation that other nations provide in combatting cybercrime, espionage, and attacks. Nations may not sign the Budapest Convention, but they can be encouraged to take additional steps to combat cybercrime and assist other nations or otherwise face negative consequences.

Greater Collaboration with Allies and Partners. In addition to combatting cybercrime, nations must also work together to decrease their vulnerability to attack and reduce the consequences of a successful attack. Collaboration on cybersecurity defenses, technology, organizations, training, and exercises across both military and civilian portions of the network is an essential step toward cybersecurity. While no defense is perfect in cyberspace, more can be done to improve upon the status quo.

On the civilian side, constant and regular engagement among U.S. and foreign Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) is a necessity.[29] Such engagement must not only occur when there is a cyber incident, but must take place regularly to ensure that all sides know their counterparts and have developed formal as well as informal relationships. This requires that the U.S. and partner CERTs/CSRITs have the resources to deal not only with the technical and information-sharing aspects of cybersecurity, but also to build relationships with cybersecurity experts in other countries. The U.S. should encourage allies to expand cyber capabilities and expand cross-border training and exercises to prepare for cyber incidents.

Beyond the response aspects, the U.S. must also seek greater cooperation with allies on cybersecurity policies and strategies. While improved technical capabilities, trust, and relationships between those in the trenches on cybersecurity are critically important, policymakers and strategists are necessary to ensure that such capabilities and relationships are advancing U.S. and allied interests and objectives. The Russians and Chinese have each developed their own ways of integrating cyber weapons and tools into their hybrid or information warfare strategies. Indeed, they do not just have strategies on paper, but are putting them to work in Ukraine, the U.S. political arena, the South China Sea, and elsewhere.

The U.S. must have a fully formed cyber strategy that includes both civilian and military components. U.S. military planners and their international partners must consider how allied forces will fight in cyberspace. In 2016, NATO declared cyberspace to be a domain of warfare in the same way that the air or the seas are.[30] Such a declaration is overdue, and

[26] Gina Stevens and Jonathan Miller, "The Obama Administration's Cybersecurity Proposal: Criminal Provisions," Congressional Research Service, July 29, 2011, p. 5, https://fas.org/sgp/crs/misc/R41941.pdf (accessed March 10, 2017).

[27] CSIS Cyber Policy Task Force, "From Action to Awareness," p. 10.

[28] Financial Action Task Force, "Improving Global AML/CFT Compliance: On-Going Process-24 February 2017," February 24, 2017, http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate) (accessed March 10, 2017).

[29] Carnegie Mellon University Software Engineering Institute, "List of National CSIRTs," http://www.cert.org/incident-management/national-csirts/national-csirts.cfm (accessed March 10, 2017).

[30] Tomáš Minárik, "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit," NATO Cooperative Cyber Defense Centre of Excellence, July 21, 2017, https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html (accessed March 10, 2017).

preparations to fight in this domain must now play catch up. NATO members and other allies must make investments in cyber capabilities that will protect and advance military objectives, in addition to much-needed investments in traditional tools of warfare. The U.S. should push for expanded partner preparation and capabilities in the domain, offering assistance where it can. Similarly, training in cyberspace and hybrid conflicts are necessary to enable the U.S. and allies to be prepared for future conflicts.

Furthermore, policymakers need to devise ways of ensuring that the private sector is also playing a leading role in cybersecurity. Government-to-government cooperation on cybersecurity must ultimately be built on private-sector expertise and control. In many countries, including the U.S., critical infrastructure is primarily owned and operated by the private sector. Even in countries where this is not true, the private sector still provides the vast majority of the goods and services, faces countless cyber attacks, and serves as the greatest repository of expertise on cybersecurity. So, any government policies on cybersecurity require true partnership with, and reliance on, the private sector. This reality should not be lost in efforts to increase cooperation between governments but should inform the way policy cooperation occurs.

Responding to Cyber Aggression

While there is much the U.S. can and should do to defend against cyber aggression both independently and in conjunction with allies and partners, the U.S. should also go beyond just defending its systems. Given the nature of cyberspace as described earlier, defense will not always succeed. When faced with an offensive-dominated domain, the U.S. can instead seek to raise the costs of hacking through various types of retaliation. These forms of retaliation should be viewed as a toolbox that can be used and tweaked depending on the aggressor to which the U.S. is responding.

Diplomatic Responses. The simplest forms of retaliation are diplomatic protests.

Naming and Shaming Bad Actors. The first step that the U.S. and all likeminded nations should take to counter nations that engage in malicious cyber behavior is naming and shaming those nations. Quite simply, the U.S. can call out nations that engage in cyber aggression and demand they stop. While unlikely to change anything on its own, when done in concert with other allies and used as a signal for further actions, diplomatic shaming is an important first step toward raising the costs of cyber aggression.

Stopping Cooperation with Bad Actors. The U.S. and its allies should also cease all forms of cyber cooperation with nations that continue to engage in blatant and widespread cyber aggression. While engagement and cooperation is valuable among friendly nations and even those that are willing to do more to combat cybercrime but simply lack the resources, cooperating with unrepentant bad actors only ignores and rewards bad behavior.

Legal and Economic Responses. *Travel and Commercial Restrictions.* For individuals and organizations that are known to be connected to the beneficiaries of malicious cyber activity, the U.S. and its allies do not need to provide them with the privilege of entering their nations on business or pleasure. The U.S. has the right to deny a visa to individuals for a variety of criminal and security reasons under section 212 of the Immigration and Nationality Act (INA).[31] For example, § 212 (f) allows the President to suspend the entry of "any alien or class of alien… [who] would be detrimental to the interests of the United States…as he may deem to be appropriate." Using §212 (f) to restrict the travel or immigration of officials or businessmen involved with or benefiting from cyber aggression would clearly be within the President's constitutional and statutory authority.[32]

Additionally, the U.S. has the right to seek commercial restrictions against businesses that represent a clear danger to critical U.S. systems or those that have a close relationship with state-sponsored hackers. For example, Huawei and ZTE are major Chinese telecommunications companies that exist and operate at the pleasure of the Chinese government, since the regime considers telecommunications to be an industry of absolute state control.[33] Given that both Huawei and ZTE have been accused of stealing intellectual

[31] U.S. Department of State, "U.S. Visas–Ineligibilities and Waivers: Laws," http://travel.state.gov/content/visas/english/general/ineligibilities.html (accessed March 10, 2017).

[32] 8 U.S. Code § 1182 (1952), Inadmissible aliens, https://www.law.cornell.edu/uscode/text/8/1182 (accessed May 18, 2017).

property and exist within a sensitive sector that could be exploited by the Chinese government, Huawei and ZTE should be restricted from operating in the U.S. at least in areas that are deemed vital to U.S. security.[34] Given that many allies, such as the United Kingdom, have conducted a substantial amount of business with these companies already, the U.S. should also investigate the risk that Chinese telecoms pose to its allies, and indirectly to the United States. This warning must not be used as a broad excuse for protectionism in other sectors where security concerns are not significant. Similarly, access to U.S. financial markets can and should exclude companies and individuals who participate in or are beneficiaries of state-sponsored cyber espionage.

Sanctions. When the U.S. has evidence that a nation-state, enterprise, or person is responsible for or involved in cyber attacks or espionage, the U.S. can pursue formal sanctions against that individual or entity. President Barack Obama, via EO 13694, created a framework for sanctions against such entities that are deemed to be

> responsible for or complicit in, or to have engaged in, directly or indirectly, cyberenabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.[35]

As is well known to many by now, President Obama expanded the scope of his original EO from incidents that harm U.S. critical infrastructure and economy to include tampering with or interfering in election processes. In December 2016, President Obama used this EO for the first time to sanction two Russian intelligence agencies and three companies, as well as four individuals connected to Russian intelligence. The EO freezes the assets of these nine entities and individuals in the U.S. and prevents them from engaging in future transactions and from visiting the U.S. Such sanctions were the right move, but were too little, too late—the U.S. should have been responding more aggressively to cyber attacks for years.[36] But now that the U.S. has finally started to use sanctions as a tool against cyber adversaries, it must build a clear record that the U.S. will respond to cyber aggression.

Legal and Criminal Charges. In cases with a significant amount of evidence pointing to individuals or organizations being directly involved in cybercrime and espionage, the U.S. can take legal action. Criminal cases based on various espionage and computer crime laws can and should be used to prosecute individuals responsible for the theft of intellectual property, proprietary information, and classified government information. The U.S. first used this tool against other nations in the cyber domain in May 2014, when it charged five members of the Chinese People's Liberation Army with stealing business secrets from U.S. corporations. While these five individuals will never see a U.S. trial, it sets a critical precedent for the U.S. to treat state-sponsored economic espionage as a crime, punishable by law. This precedent could be applied in the future to other individuals or companies that are not in China but are found across the world and in the U.S. If a company assists with and receives information and tangible benefits from a state-sponsored campaign of economic espionage, the U.S. can pursue cases to seize that company's assets or jail its executives that are within the reach of U.S. or allied authorities.

[33] Zhao Huanxin, "China Names Key Industries for Absolute State Control," *China Daily*, December 19, 2006, http://www.chinadaily.com.cn/china/2006-12/19/content_762056.htm (accessed May 31, 2017).

[34] Derek Scissors and Steven Bucci, "China Cyber Threat: Huawei and American Policy Toward Chinese Companies," Heritage Foundation *Backgrounder* No. 3761, October 23, 2012, http://www.heritage.org/research/reports/2012/10/china-cyber-threat-huawei-and-american-policy-toward-chinese-companies.

[35] U.S. Treasury, "Presidential Documents, Executive Order 13757, 2016," *Federal Register*, December 28, 2017, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber2_eo.pdf (accessed May 18, 2017).

[36] David Inserra, "U.S. Should Stand Up to China on Cyber Attacks," The Daily Signal, May 1, 2013, http://dailysignal.com/2013/05/01/u-s-should-stand-up-to-china-on-cyber-attacks/; David Inserra and Ellen Prichard, "Suspected Russian Penetration of U.S. Critical Infrastructure Calls for Firm Response," The Daily Signal, November 10, 2014, http://dailysignal.com/2014/11/10/suspected-russian-penetration-u-s-critical-infrastructure-calls-firm-response/; and David Inserra and Jennifer Guthrie, "Cyber Breach at the White House: Time to Increase Cyber Defenses and Detect Cyber Aggression," The Daily Signal, April 9, 2015, http://dailysignal.com/2015/04/09/cyber-breach-at-the-white-house-time-to-increase-cyber-defenses-and-deter-cyber-aggression/.

Such cases also show malicious cyber nations that the U.S. will not sit idly by, but will protect its companies and interests. This not only acts as a warning to bad actors, it also sends a positive message to U.S. businesses that the U.S. government is willing to support and defend them. Having other nations join the U.S. in this effort would place a great deal of pressure on individuals and companies that are connected to state-sponsored cyber economic espionage.

World Trade Organization (WTO) Action. For states that systematically support or engage in espionage or cybercrime against other nation's businesses, the U.S. and its allies may have grounds to seek WTO relief.

In the cybersecurity, trade, and legal communities, there are different opinions over whether hacking and economic espionage by nation-states, such as China, break WTO rules.[37] Specifically, the issue in many debates seems to be that "WTO rules create obligations for WTO members to fulfill within their territories and do not generally impose duties that apply outside those limits," such that China only has an obligation to stop economic espionage on U.S. companies in China, not espionage that occurs in the U.S.[38]

There are, however, other provisions of trade law and convention to which most countries, including the main cyber antagonists, China and Russia, are signatories.[39] Specifically, as a member of the WTO, a nation is a signatory to the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS), which requires each nation to uphold certain basic principles regarding the protection of intellectual property.[40] The TRIPS agreement has two articles that could be used by the U.S. and other nations to retaliate against nations like China or Russia for their cyber aggression:

1. The TRIPS Article 73, "Security Exceptions." The last provision of TRIPS allows a nation to take any action that it feels is "necessary for the protection of its essential security interests," or for the "maintenance of international peace and security." Using such a provision, however, would set a dangerous precedent that other nations could use as well, thus likely starting tit-for-tat trade wars.

2. TRIPS Article 2, "Unfair Competition." According to Article 2 of TRIPS, all signatories of TRIPS are required to uphold various articles of the Paris Convention including Article 10, which reads:

> Unfair Competition
> (1) The countries of the Union are bound to assure to nationals of such countries effective protection against unfair competition.
> (2) Any act of competition contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition.

This text specifies a treaty obligation that many state sponsors of economic espionage are not keeping. After all, stealing trade information, whether through traditional economic espionage or cyber espionage, and then giving this information to domestic companies for their use appears to neatly fit the definition provided in (2) above. Furthermore, to counter the arguments that WTO rules do not apply here, it would seem that such a standard, even if only "creat[ing] obligations for WTO members to fulfill within their territory," still presents an obligation to stop state-sponsored hackers from engaging in widespread campaigns to steal business and trade secrets and profit from them, which would be unfair competition.

[37] FierceTechExec, http://www.fiercegovernmentit.com/story/lewis-us-should-go-wto-over-chinese-espionage/2013-02-11 (accessed May 18, 2017), and David P. Fidler, "Economic Cyber Espionage and International Law: Government Acquisition of Trade Secrets Through Cyber Technologies," *Insights*, Vol. 17, No. 10 (March 20, 2013), https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving (accessed March 10, 2017).

[38] World trade Organization, "Understanding the WTO: The Agreements," http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm1_e.htm (accessed May 11, 2017), and Fidler, "Economic Cyber Espionage and International Law."

[39] World Trade Organization, "Members and Observers," http://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm (accessed May 11, 2017).

[40] World Trade Organization, "Overview: The TRIPS Agreement," https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm (accessed May 11, 2017).

If a nation is not meeting its obligations under TRIPS and the Paris Convention, the U.S. can pursue legal action per Part 5 of TRIPS, which refers to Articles 22 and 23 of the 1994 General Agreement on Tariffs and Trade and the dispute-settlement procedures it established.[41] Of course, this may require the U.S., other countries, and businesses to publicly disclose information that may reveal sources and methods of intelligence and security. This process is already beginning with private-sector cybersecurity agencies revealing technical security details in order to incriminate advanced persistent threats (APT) as seen in the Mandiant Report about APT 1 in early 2013 and many subsequent reports.[42] Additionally, with the U.S. charging Chinese military officers with hacking in May 2014, the government has shown itself willing to lay out its technical and legal case against bad actors.

Of course, being able to legally prove in the WTO dispute-settlement process that any specific hacking event was part of a campaign of economic espionage would be difficult. But attribution, as mentioned, is not impossible, and a consistent and coordinated effort by the U.S. government and other nations that are victims of economic espionage could yield a strong, united WTO case against the Chinese, Russians, and other bad actors.

Before entering into a WTO dispute and preparing its case, the U.S. should also understand its objective. Should the U.S. win its case (and assuming the bad actor does not immediately take legitimate action to fix its transgressions), there are at least two outcomes the U.S. could seek through the WTO.

First, the U.S. could simply seek the moral high ground and diplomatic victory accompanying a verdict that a nation's systematic economic hacking is contrary to it legal obligations through the WTO. Perhaps one of the strongest forms of naming and shaming, a collection of nations winning a WTO case against a nation engaging in economic espionage would be a major diplomatic victory. This decision could unite other nations against the offending nation and be used to leverage broader and more robust punitive measures.

Second, the U.S. could seek a WTO remedy, retaliation that is meant to bring the offending nations into compliance. Such a remedy could take several forms, including a significant increase in U.S. and other nations' tariffs on certain goods from the offending nation[43] or suspension of certain intellectual property (IP) right protections for the offending nation's goods. The U.S. must be careful with such tools, especially the use of tariffs, as the U.S. benefits from trade, and raising the price of goods would also be harmful to U.S. consumers. It is also unlikely that all the nations that stood with the U.S. in the WTO would agree to place tariffs on certain goods, lessening the force of such retaliation. Despite such realities, tariffs should remain on the table as long as they are used in a manner that seeks to correct offending behavior.

An alternative retaliation, suspending IP protections[44] for certain goods provided by the offending nation, is in many ways the most reciprocal form of retaliation, since economic espionage is usually aimed at stealing IP. The offending nation's affected goods and companies would suffer serious reputation and legal damage, risking long-term damage to the sale and use of its goods, as well as future innovation. As with tariffs, there could also be harm to U.S. consumers and producers that must then navigate a market with protected and non-protected goods. This damage could be somewhat offset by the fact that U.S. producers can use relevant IP for their own benefit. The IP of some nations might be limited, which also limits the effectiveness of an IP-protection suspension.

Regardless, should the U.S. and its partners win a WTO judgment, they should use the available tools judiciously to encourage a change in the offending nation's behavior, while avoiding harmful side effects to consumers and producers.

[41] World Trade Organization, "General Agreement on Tariffs and Trade 1994," https://www.wto.org/english/docs_e/legal_e/06-gatt_e.htm (accessed May 11, 2017).

[42] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (accessed May 11, 2017).

[43] World Trade Organization, "Understanding the WTO: Settling Disputes," https://www.wto.org/english/thewto_e/whatis_e/tif_e/disp1_e.htm (accessed May 11, 2017).

[44] Henning Grosse Ruse-Khan, "Suspending IP Obligation Under TRIPS: A Viable Alternative to Enforce Prevailing WTO Rulings?" Center for International Environmental Law, April 2008, http://www.ciel.org/Publications/TRIPS_IP_7May08.pdf (accessed May 11, 2017).

Strategic Responses. Finally, some nations may only be deterred from cyber aggression if they feel pressure on more fundamental issues, which differ from country to country. Territorial disputes, invasions, or other threats to democratic rule, such as Ukraine and Georgia in the case of Russia, and Taiwan and Hong Kong in the case of China, provide examples of pressure points that the U.S. can use to retaliate against cyber aggression. Standing up for Taiwan, Hong Kong, Ukraine, Georgia, and other countries is not only a good response to unrepentant cyber aggressors, but also important to U.S. foreign policy in general. More specifically, an example of a strategic response in Russia's case might be supporting Ukraine's defense of its territory through arms sales. Not only is it a unique way of responding to Russian actions in cyberspace, it also provides the U.S. a specific response to Russian aggression in Eastern Europe. Using these pressure points appropriately, tailored to the aggressor, provides the U.S. with some of its most powerful tools to retaliate against nation-states.

Another example of a strategic response that hits close to home is Internet freedom. States like Russia and China also depend on repression and censorship to maintain control of their populations, albeit using different techniques. While "democracy promotion" may seem to be a relatively minor activity, and one that the U.S. should be engaged in regardless of the threat, this policy option more than passively, indirectly, or softly supports democratic movements in authoritarian nations. In this context, democracy promotion includes a substantial increase in public, diplomatic, financial, and legal support for organizations and individuals that seek dramatic democratic reforms and challenge governments that do not respect individual liberty, the rule of law, or the right to vote for an opposition government.

Such policies directly challenge these authoritarian regimes, striking at their monopoly on power and information. At its most basic form, this means using U.S. public diplomacy to counter the growing tide of Chinese and Russian propaganda. With China and Russia doing all they can to portray themselves and their actions as legitimate and positive, the U.S. needs to return its public diplomacy measures to where they were in the 1980s, when the U.S. discredited the Soviet Union with audiences across the world, including within the Soviet Union.[45] Sadly, U.S. public diplomacy fell into disrepair after the Cold War, as peace dividends and reorganizations claimed the effectiveness of this great tool. On the other hand, Russia and China actively challenge U.S. policies and leadership through their propaganda forces. The Russian and Chinese efforts in this arena are met with limited or ineffective responses from the U.S.

This must change—the U.S. must actively counter such propaganda both around the world and within these countries. Public diplomacy programs, such as the Voice of America, allow the U.S. to effectively promote a better image of the United States while countering anti-U.S. campaigns. To be more effective in countering anti-U.S. propaganda, U.S. broadcasts should be reformed, with operations manned by individuals dedicated to the U.S. and her values and with broadcasts that do not merely provide news but also include staunch support of U.S. policies and values.[46] The U.S. should not be in the business of merely paying for another source of news—it should actively promote U.S. policies and principles while sharing news about the world from the U.S. perspective. Research into, and collection of, best practices in public diplomacy should be jump-started. Embassy officials should receive uniform guidance on how to more directly challenge disinformation and spread the truth about U.S. policies, as well as the truth about repression within various regions.[47]

Going further, the U.S. should take a more active role in supporting dissidents and democratic activists. Such action also requires that U.S. public diplomacy mechanisms be reinvigorated. By using a variety of mediums, including radio, television, and the Internet, the U.S. can provide dissidents in repressive states with information and support. Radio Free Asia and the Broadcasting Board of Governors can

[45] Helle Dale, Ariel Cohen, and Janice Smith, "Challenging America: How Russia, China, and Other Countries Use Public Diplomacy to Compete with the U.S.," Heritage Foundation *Backgrounder* No. 2698, June 21, 2012, http://www.heritage.org/research/reports/2012/06/challenging-america-how-russia-china-and-other-countries-use-public-diplomacy-to-compete-with-the-us.

[46] Helle Dale, "A Snub to Congress: Oversight of International Broadcasting Agency in Question," The Daily Signal, September 20, 2014, http://dailysignal.com/2014/09/26/snub-congress-oversight-international-broadcasting-agency-question/.

[47] Dale, Cohen, and Smith, "Challenging America."

more aggressively spread information and broadcasts and supply dissidents with technology that allows them to communicate with others and protect themselves from the prying eyes of the Chinese censors and police. The U.S. can offer similar tools, information, and protections to critics of Vladimir Putin through Radio Free Europe/Radio Liberty.[48] The U.S. must also use its foreign aid appropriately to support pro-democracy and civil society programs and organizations. The U.S. is already accused of interfering in these nations[49]—it might as well take the blame and forcefully support those who desire freedom, the rule of law, and basic human rights.[50]

While these policies may be among the most strategic the U.S. could undertake, the use of all other tools should also be considered strategically. Some countries may not care about diplomatic repercussions, while others may not be greatly affected by legal consequences, limiting the usefulness of such tools to counter cyber aggression. Responding to bad cyber actors requires moving beyond cyberspace, using the full range of national power to tailor responses that are most likely to deter or punish their cyber aggression.

All Tools of National Power Needed

These policy options are just that—options. Very few circumstances call for action at the WTO or the use of serious strategic responses. In fact, in most cases, cooperation with other nations on beefing up cybersecurity and the enforcement of cybercrime laws is the most appropriate answer. Indeed, the U.S. needs to do many things to improve its international cybersecurity. While most of the responsibility for these actions falls to the Administration, Congress can also demand that certain actions, such as sanctions, be taken against bad actors. To that end, Congress and the Administration should:

- **Deepen collaboration on cybercrime among like-minded nations.** The U.S. should look to create an acceptance for active cyber defenses that are not harmful, but allow better attribution of, and intelligence on, cyber threats. Laws and tools from the organized crime arena, such as RICO, should be expanded to cover TCOs engaging in cybercrime.

- **Expand cybercrime cooperation beyond current signatories of the Budapest Convention.** The U.S. should create a cyber form of the FATF that combats money laundering and financing of terrorism. While they need not abide by all the terms of the Budapest Convention, non-signatory countries should still be pressured to take reasonable actions against cybercrime. Nations that do not assist in international cybercrime investigations, or do little to stop cybercrime within their territories, should be considered non-cooperative and face repercussions from members of the new cyber task force.

- **Improve cooperation with foreign civilian cybersecurity defense and response organizations.** Beyond defeating cybercrime, the U.S. must also establish more regular interactions and cooperation with CERTs and CSIRTs of partners and allies to bolster cyber defenses. This means increasing cross-border information sharing and joint training and exercises for civilian security organizations.

- **Prepare to fight in the cyber domain with allies.** The U.S. and its allies also need to develop the tools and capabilities to fight in the cyber domain. While NATO has taken some steps in this direction, far more needs to be done. Any future conflict will require offensive and defen-

[48] Daniel Kochis, "Countering Russian Propaganda Abroad," Heritage Foundation *Backgrounder* No. 4286, October 21, 2014, http://www.heritage.org/research/reports/2014/10/countering-russian-propaganda-abroad.

[49] David M. Herszenhorn and Ellen Barry, "Russia Demands U.S. End Support of Democracy Groups," *The New York Times*, September 18, 2012, http://www.nytimes.com/2012/09/19/world/europe/russia-demands-us-end-pro-democracy-work.html?pagewanted=all&_r=1& (accessed March 10, 2017); Elise Labott, "China Accuses U.S. of Interference," CNN, February 26, 2009, http://www.cnn.com/2009/POLITICS/02/26/china.state/index.html?iref=24hours (accessed March 10, 2017); and Sneha Shankar, "China Condemns US for Distorting Facts About Protests, Asks It to Stop Interfering," *International Business Times*, October 10, 2010, http://www.ibtimes.com/china-condemns-us-distorting-facts-about-hong-kong-protests-asks-it-stop-interfering-1702743 (accessed March 10, 2017).

[50] Dean Cheng and Ariel Cohen, "How Washington Should Manage U.S.–Russia–China Relations," Heritage Foundation *Backgrounder* No. 2841, August 29, 2013, http://www.heritage.org/global-politics/report/how-washington-should-manage-us-russia-china-relations.

sive cyber capabilities that are well integrated into U.S. and allied warfighting strategies. Creating such capabilities requires a political will to engage in this new domain as well as the resources to develop the means of engagement.

- **Develop a robust policy of deterrence that tailors a proportionate U.S. response to the bad actors.** Deterrence is in the mind of the adversary—he chooses to alter his behavior because he believes the costs are too high. The only way to achieve deterrence in cyberspace is to establish a clear pattern of policy and action that leads an actor to rethink his plans. The U.S. has a whole host of tools it can use to retaliate against any sort of cyber aggression, including diplomatic naming and shaming, cutting off cooperation, visa restrictions, commercial and financial limitations, sanctions, legal action, trade enforcement tools, action on other military or foreign policy matters, support to dissidents in malicious cyber states, and other tools not considered here. These tools should be used in a way that is tailored to fit the adversary and proportionate to the scale and effects of his aggressive action.

- **Create a new strategy for international efforts in cyberspace.** The U.S. needs to articulate a bolder strategy for how it will operate in the cyber domain. From deterring and retaliating against cyber aggressors to reinforcing cybercrime defense efforts with allies, the U.S. should craft a new strategy that will direct the whole of government to protect U.S. interests in cyberspace. This strategy must also consider the central role the private sector plays and make use of its expertise and skills.

Using the Right Tools at the Right Time

It is past time for the U.S. to take the lead on international cybersecurity. Cybercrime harms people around the globe, state-sponsored economic espionage harms the creative and innovative private sector, and state-led attacks on political organs undermine faith in institutions and the authenticity of news. While criminals and certain nation-states may benefit from this, the vast majority of nations, companies, and individuals lose. The U.S. must take action to defend itself in cyberspace through cooperation with like-minded partners while deterring those that benefit from cybercrime and warfare. Doing so will make the U.S. and its allies safer, more prosperous, and freer.

*—**David Inserra** is a Policy Analyst for Homeland Security and Cyber Security in the Douglas and Sarah Allison Center for Foreign and National Security Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*