How Should the U.S. Respond to a Russian Cyber Attack?

By Nicole Softness

Following the hacking of the Democratic National Committee in 2016, the United States publicly expressed concern that it could imminenty face additional cyber attacks. Public discourse has focused on Russia as a likely culprit, calling attention to its advanced military technology in Syria, President Vladimir Putin's prioritization of information warfare, and its deteriorating relationship with the United States. A historical analysis of Russia's strategic military choices suggests that the state would prioritize the U.S. information technology (IT) and communications critical infrastructure as key cyber targets. In reaction to such an attack, the United States would have to choose from a spectrum of military and intelligence counter-responses, ranging from lower-level alternatives to those with high potential for escalation.

POLITICAL LANDSCAPE

Recent attribution reports by private cyber security firms CrowdStrike and Mandiant allege that Russia conducted the 2015-2016 hacks on the Democratic National Committee (DNC). Citing weak international cyber norms, the Obama administration argued that Russia has violated what all responsible nations would consider acceptable state behavior. In the absence of an immediate response to these violations, and the lengthy attribution process, the American population has arguably become complacent, especially considering minimal military responses to other publicized cyber intrusions (i.e., Sony Pictures, and the Office of Personnel Management). Admiral Michael S. Rogers, Director of the National Security Agency (NSA) and U.S. Cyber Command, believes that this complacency will only vanish if a cyber attack on U.S. soil achieves large-scale destruction.

RUSSIAN STRATEGY AND CAPABILITIES

The U.S. Intelligence Community's 2015 Worldwide Threat Assessment highlighted China and Russia as the "most sophisticated nation-state actors" in the new generation of cyber warfare and noted that Russian hackers have impressive programming power and inventiveness. With the exception of the U.S. Stuxnet incident, Russia is the only state that has publicly successfully augmented cyber warfare with conventional warfare, evidenced when Russian hackers manipulated blast furnace control systems in a German steel mill in 2014; conducted cyber-to-conventional operations against Georgia in 2008; and interfered with a French blast furnace control systems in a German steel mill in 2014; conducted cyber-to-conventional operations against Georgia in 2008; and interfered with a French...
Strategically, Russia has an incentive to employ its cyber arsenal to further its broader political aims.

In order to achieve this strategic preparation, Russia could choose from an array of cyber tools, possessed by two prominent hacker groups, APT29 and APT28. According to NATO, APT29 has successfully spear phished information related to Russian geopolitical interests, while APT28 has targeted European states. In 2008, Russia was able to manipulate its IP addresses with Agent BTZ to penetrate U.S. military networks, and throughout 2013-2014, used highly complex malware to penetrate Ukraine. In 2014, researchers discovered that this malware, called television network, the Polish stock market, and the U.S. State Department. This intent and capability to supplement cyber intrusions with conventional consequences demonstrates the unique and serious character of the Russian cyber threat.

Russia's political elite has prioritized these capabilities. The Henry Jackson Society, a British-based think tank, wrote in 2016 that, “as far as the Kremlin is concerned, geeks and hackers now rank alongside soldiers and spies as weapons of the state.”7 Russian military and academic elites have published a plethora of documents over the past decade describing the state's desires to modernize its information warfare defenses and capabilities, as well as its strategy of utilizing cyber means to disrupt its enemy's weapons, decision makers, and the minds of average citizens.8 The information-psychological aspects of information warfare have an integral role within the strategies of these documents, demonstrating the possibility that Russia could contextualize an attack within a greater emergency context, in the hopes of causing disorganization within the American citizenry, resulting in panic or loss of life.9 These leaked policies, along with Russia's history of attacks, demonstrate clearly significant cyber capabilities, and willingness to target critical industries.

Strategically, Russia has an incentive to employ its cyber arsenal to further its broader political aims. A 2015 NATO report noted Russia's unique ability to foresee the broader impact of technology on the field of battle, and the military advantage of using cyber attacks to “intensify the fog of war.”10

Russia is not likely to target something without an end goal; rather, the state would aim to confuse the United States just enough to force it to begin and escalate a low-level cyber conflict. This strategy of pepping the battlefield is consistent with Russia's strategy during the Cold War, when operatives constructed maps of U.S. cities for future exploitation. Within the scope of cyber, this strategy would translate to Russian intelligence operations conducted against the United States, with the goal of acquiring information related to activities in Ukraine and Syria, U.S. military operations, and to generally "prepare the cyber environment for contingencies."11

In order to achieve this strategic preparation, Russia could choose from an array of cyber tools, possessed by two prominent hacker groups, APT29 and APT28. According to NATO, APT29 has successfully spear phished information related to Russian geopolitical interests, while APT28 has targeted European states.12 In 2008, Russia was able to manipulate its IP addresses with Agent BTZ to penetrate U.S. military networks, and throughout 2013-2014, used highly complex malware to penetrate Ukraine.13 In 2014, researchers discovered that this malware, called
Targeted Zero-Days [the early acquisition, via purchase or discovery, of software vulnerabilities largely in email attachments, to infect energy and telecommunications firms, as well as government targets.]\(^{16}\)

RUSSIAN CYBER ATTACKS ON THE UNITED STATES

Russia's past strategic choices, demonstrate an unwillingness to commit an act that could trigger a full-scale war, potentially with nuclear weapons. The country's focus on battlefield preparation and intelligence gathering suggests that strategies would work to take advantage of U.S. complacency via the preponderance of smaller-scale cyber attacks, and would conduct an attack unlikely to trigger a full-scale military response. By choosing an industry with consequences limited to the United States, Russia could avoid damaging its alliances or inciting other states to join forces against Russia militarily, politically, or economically. According to this analysis, Russia would choose not to conduct a cyber attack on the majority of the United States’ critical infrastructure sectors, for fear of over-escalation.\(^{15}\) Attacks on the defense, nuclear, and chemical sectors could be immediately considered acts of war, while attacks on the financial, food and agricultural, or critical manufacturing sectors would be likely to enrage other states dependent on the United States for economic stability. Thus, with these strategic choices and toolkits in mind, if Russia were to conduct a cyber-to-conventional attack against the United States, it would choose to target either the communications or IT critical infrastructure sectors.

A Russian attack on these sectors could take several forms. Russia could use any of the following tools to cause serious damage to U.S. operations:

- Social engineering [taking advantage of human vulnerabilities to dismantle cyber security]
- Counterfeit devices [the replacement of crucial technology with unapproved, alternative products]
- Targeted Zero-Days [the early acquisition, via purchase or discovery, of knowledge regarding system vulnerabilities, and the ability to act early on those vulnerabilities]
- Exploits [Identifying vulnerabilities, and using tools to break into systems and alter, steal, or block data].\(^{16}\)

In the past, Russian cyber operations against the United States manifested largely as simple procedures, requiring little financial and operational support. Throughout 2014 and 2015, Russia employed more complex strategies against government computers, including “disguising the electronic ‘command and control’ messages that set off alarms for anyone looking for malicious actions.” This precedent for attacking alert systems demonstrates that even robust U.S. monitoring systems could have trouble catching Russian intrusions within the necessary window to stop or identify the hack. “If the adversaries know you are aware of their presence, they will take steps to burrow in, or erase the logs that show they were present,” said Michael Sussman of Perkins Coie LLP.\(^{18}\)

Sandworm, had used zero-day exploits, software vulnerabilities largely in email attachments, to infect energy and telecommunications firms, as well as government targets.\(^{16}\)

RUSSIAN CYBER ATTACKS ON THE UNITED STATES

Russia's past strategic choices, demonstrate an unwillingness to commit an act that could trigger a full-scale war, potentially with nuclear weapons. The country's focus on battlefield preparation and intelligence gathering suggests that strategies would work to take advantage of U.S. complacency via the preponderance of smaller-scale cyber attacks, and would conduct an attack unlikely to trigger a full-scale military response. By choosing an industry with consequences limited to the United States, Russia could avoid damaging its alliances or inciting other states to join forces against Russia militarily, politically, or economically. According to this analysis, Russia would choose not to conduct a cyber attack on the majority of the United States’ critical infrastructure sectors, for fear of over-escalation.\(^{15}\) Attacks on the defense, nuclear, and chemical sectors could be immediately considered acts of war, while attacks on the financial, food and agricultural, or critical manufacturing sectors would be likely to enrage other states dependent on the United States for economic stability. Thus, with these strategic choices and toolkits in mind, if Russia were to conduct a cyber-to-conventional attack against the United States, it would choose to target either the communications or IT critical infrastructure sectors.

A Russian attack on these sectors could take several forms. Russia could use any of the following tools to cause serious damage to U.S. operations:

- Social engineering [taking advantage of human vulnerabilities to dismantle cyber security]
- Counterfeit devices [the replacement of crucial technology with unapproved, alternative products]
- Targeted Zero-Days [the early acquisition, via purchase or discovery, of knowledge regarding system vulnerabilities, and the ability to act early on those vulnerabilities]
- Exploits [Identifying vulnerabilities, and using tools to break into systems and alter, steal, or block data].\(^{16}\)

In the past, Russian cyber operations against the United States manifested largely as simple procedures, requiring little financial and operational support. Throughout 2014 and 2015, Russia employed more complex strategies against government computers, including “disguising the electronic ‘command and control’ messages that set off alarms for anyone looking for malicious actions.” This precedent for attacking alert systems demonstrates that even robust U.S. monitoring systems could have trouble catching Russian intrusions within the necessary window to stop or identify the hack. “If the adversaries know you are aware of their presence, they will take steps to burrow in, or erase the logs that show they were present,” said Michael Sussman of Perkins Coie LLP.\(^{18}\)
If the Russian strategy of doxing, or broadcasting stolen intelligence, was meant to disrupt U.S. politics and intensify the fog of war, then the Russians would have achieved their goal, and would be likely to repeat this tactic against government executives within the communications and IT industries.

Russia could graduate from doxing and focus on tactics with more immediate conventional consequences. By targeting central systems within the IT and communications industries, using DDoS attacks or stealing information that could cripple internal proceedings, Russia could disrupt service for thousands of phone customers or sever the Internet for millions of consumers. It could also shut down government IT operations during wartime, or disrupt national emergency alert services, including 911 networks or emergency broadcast stations, during a national disaster. The latter scenarios could cause immense economic and military harm to the United States and even result in loss of life and safety.

There are an overwhelming number of vulnerabilities within these systems. The communications sector is inextricably linked with the energy, IT, banking and finance, postal and shipping, and emergency services sectors, while the IT sectors provide control systems, technology and Internet infrastructure, and operating systems for all major military and civilian networks. These systems present additional vulnerabilities to Russian cyber actors, as a majority of their operations lack government oversight.

A huge number of nodes within the United States’ critical communications systems are managed by private companies, such as FOX, which have private sector-driven priorities, and could not ostensibly perform seamless defensive cyber security collaborations with the government. This lack of centralization is a clear challenge for national defense. Although these companies certainly have incentives to implement sufficient security features, they are for-profit organizations. The National Telecommunication and Information Administration (NTIA) cautioned in 2013 that these infrastructure operators “would invest in cyber security to a level that is justifiable according to their own business plans – this is a unique warfare threat – we have private companies responsible for determining budgets for issues of national security.”

However, notwithstanding profit-based priorities, private companies also have a significantly larger cyber security arsenal than the government. Over five years, the private sector doubled its spending on cyber security from $40 billion to $80 billion, while the Department of Homeland Security, specifically tasked with defending the United States on the ground and in cyberspace, received a mere $39 billion in additional vulnerabilities to Russian cyber actors, as a majority of their operations lack government oversight.

Russia could graduate from doxing and focus on tactics with more immediate conventional consequences. By targeting central systems within the IT and communications industries, using DDoS attacks or stealing information that could cripple internal proceedings, Russia could disrupt service for thousands of phone customers or sever the Internet for millions of consumers. It could also shut down government IT operations during wartime, or disrupt national emergency alert services, including 911 networks or emergency broadcast stations, during a national disaster. The latter scenarios could cause immense economic and military harm to the United States and even result in loss of life and safety.

There are an overwhelming number of vulnerabilities within these systems. The communications sector is inextricably linked with the energy, IT, banking and finance, postal and shipping, and emergency services sectors, while the IT sectors provide control systems, technology and Internet infrastructure, and operating systems for all major military and civilian networks. These systems present additional vulnerabilities to Russian cyber actors, as a majority of their operations lack government oversight.

A huge number of nodes within the United States’ critical communications systems are managed by private companies, such as FOX, which have private sector-driven priorities, and could not ostensibly perform seamless defensive cyber security collaborations with the government. This lack of centralization is a clear challenge for national defense. Although these companies certainly have incentives to implement sufficient security features, they are for-profit organizations. The National Telecommunication and Information Administration (NTIA) cautioned in 2013 that these infrastructure operators “would invest in cyber security to a level that is justifiable according to their own business plans – this is a unique warfare threat – we have private companies responsible for determining budgets for issues of national security.”

However, notwithstanding profit-based priorities, private companies also have a significantly larger cyber security arsenal than the government. Over five years, the private sector doubled its spending on cyber security from $40 billion to $80 billion, while the Department of Homeland Security, specifically tasked with defending the United States on the ground and in cyberspace, received a mere $39 billion in...
2012 for all of its programs. However, the NTIA has argued that even this large private sector budget cannot account for and prevent “remote cyber threats,” which make up the majority of attacks. Cyber attacks are much harder to anticipate than conventional attacks, and it is never immediately clear what caliber defense will be required to slow the said attack, or trace the attack back to its origins for future countermeasures.

**U.S. DEFENSE CAPABILITIES**

In 2013 the United States published the National Infrastructural Protection Plan, which included defense strategies and implementations for each critical infrastructure sector. The plan assessed sector-specific vulnerabilities and risk profiles, likely targets, and methods of addressing those vulnerabilities. These methods include several priorities for passive and active protections. Under the plan, the government must perform continuous monitoring and diagnoses of all CI cyber systems, and conduct immediate information sharing during and after all cyber incidents. Sectors must also back up essential information on remote servers disconnected from the Internet, to ensure redundancy in the case of attack. Over time, key operational functions must be removed from Internet-connected networks, to ensure that any incidents can be sufficiently contained from public consequences.

**DEFENSE SCOPE OF COMMUNICATIONS AND IT SECTORS**

The communications sector represents a large host of attack vulnerabilities. In 2014, Information and Communications Technology (ICT) accounted for 3.5 million jobs, and $1 trillion of the U.S. GDP (7 percent of the economy). This cyber infrastructure includes access networks, and thousands of cable systems, satellites, and wireless networks. Russia could specifically capitalize on these opportunities by targeting private-sector-managed gaps within the industry’s supply chains, including:

- Power and data sources [Physical infrastructures such as data centers provide energy and information to networks that serve millions of consumers.]
- Diesel fuel centers for generators [These fuel centers keep generators alive, and allow for systems to transport data between different areas of the network.]
- Fuel transportation [Roads and trucks are required to transport physical infrastructure crucial to maintaining IT and communications networks open, and are thus vulnerable as physical, isolated, and moving targets.]
- Technological products [Communications and IT networks depend on physical pieces of technology to move and retain information between computers and other devices, such as routers, as well as software that automates crucial government processes.]

2012 for all of its programs. However, the NTIA has argued that even this large private sector budget cannot account for and prevent “remote cyber threats,” which make up the majority of attacks. Cyber attacks are much harder to anticipate than conventional attacks, and it is never immediately clear what caliber defense will be required to slow the said attack, or trace the attack back to its origins for future countermeasures.

**U.S. DEFENSE CAPABILITIES**

In 2013 the United States published the National Infrastructural Protection Plan, which included defense strategies and implementations for each critical infrastructure sector. The plan assessed sector-specific vulnerabilities and risk profiles, likely targets, and methods of addressing those vulnerabilities. These methods include several priorities for passive and active protections. Under the plan, the government must perform continuous monitoring and diagnoses of all CI cyber systems, and conduct immediate information sharing during and after all cyber incidents. Sectors must also back up essential information on remote servers disconnected from the Internet, to ensure redundancy in the case of attack. Over time, key operational functions must be removed from Internet-connected networks, to ensure that any incidents can be sufficiently contained from public consequences.

**DEFENSE SCOPE OF COMMUNICATIONS AND IT SECTORS**

The communications sector represents a large host of attack vulnerabilities. In 2014, Information and Communications Technology (ICT) accounted for 3.5 million jobs, and $1 trillion of the U.S. GDP (7 percent of the economy). This cyber infrastructure includes access networks, and thousands of cable systems, satellites, and wireless networks. Russia could specifically capitalize on these opportunities by targeting private-sector-managed gaps within the industry’s supply chains, including:

- Power and data sources [Physical infrastructures such as data centers provide energy and information to networks that serve millions of consumers.]
- Diesel fuel centers for generators [These fuel centers keep generators alive, and allow for systems to transport data between different areas of the network.]
- Fuel transportation [Roads and trucks are required to transport physical infrastructure crucial to maintaining IT and communications networks open, and are thus vulnerable as physical, isolated, and moving targets.]
- Technological products [Communications and IT networks depend on physical pieces of technology to move and retain information between computers and other devices, such as routers, as well as software that automates crucial government processes.].
The IT sector, while similar to the scope of the communications sector, includes newer “trends” in vulnerabilities that are open to attack, including an increasing reliance on the Internet of Things (IoT), cloud computing, and mobile computing. Likely targets for a cyber attack within this sector could include:

- Internet routers
- Domain Name System (DNS) operators
- Supply chains (distribution of untrustworthy content via these vulnerabilities)
- Internet Service Providers (ISP) (could block Internet activity)
- Security vendors.

In recognition of these vulnerabilities, and the disastrous consequences that could result from an attack on each critical node, the government conducts continuous aggressive active defenses on behalf of each of these sectors, and continuously looks for intrusions, suspicious activity, or alterations in content. These active defenses include information sharing, technical tools that slow hackers at the perimeter (tarpits and honeypots), denial and deception (providing false information in front of legitimate information), beacons (software hidden in files that sends an alert in response to unauthorized access), hunting (rapidly enacted technical measures that evict adversaries already present in a network), intelligence gathering in the Deep Web and Dark Net (continuous and covert human intelligence to identify likely adversaries and toolkits), and white-hat ransomware (legal malware utilized by public-private partners to obtain stolen information and return it to proper owners).

**GOVERNMENT ORGANIZATION FOR A CYBER ATTACK**

In 2016, under the mandate of Presidential Policy Directive (PPD) 41 – United States Cyber Incident Coordination, the White House released the definition of a significant cyber attack as something “likely to result in demonstrable harm to national security interests, foreign relations, the domestic and global economy, public confidence, civil liberties, or public health and the safety of the American people.”

A Russian cyber attack on communications or IT critical infrastructure, particularly in the context of a national emergency, would fall under this classification.

In the event of such an attack, the United States would draw together the National Cyber Response Group, which would lead the defensive response in support of

---

The IT sector, while similar to the scope of the communications sector, includes newer “trends” in vulnerabilities that are open to attack, including an increasing reliance on the Internet of Things (IoT), cloud computing, and mobile computing. Likely targets for a cyber attack within this sector could include:

- Internet routers
- Domain Name System (DNS) operators
- Supply chains (distribution of untrustworthy content via these vulnerabilities)
- Internet Service Providers (ISP) (could block Internet activity)
- Security vendors.

In recognition of these vulnerabilities, and the disastrous consequences that could result from an attack on each critical node, the government conducts continuous aggressive active defenses on behalf of each of these sectors, and continuously looks for intrusions, suspicious activity, or alterations in content. These active defenses include information sharing, technical tools that slow hackers at the perimeter (tarpits and honeypots), denial and deception (providing false information in front of legitimate information), beacons (software hidden in files that sends an alert in response to unauthorized access), hunting (rapidly enacted technical measures that evict adversaries already present in a network), intelligence gathering in the Deep Web and Dark Net (continuous and covert human intelligence to identify likely adversaries and toolkits), and white-hat ransomware (legal malware utilized by public-private partners to obtain stolen information and return it to proper owners).

**GOVERNMENT ORGANIZATION FOR A CYBER ATTACK**

In 2016, under the mandate of Presidential Policy Directive (PPD) 41 – United States Cyber Incident Coordination, the White House released the definition of a significant cyber attack as something “likely to result in demonstrable harm to national security interests, foreign relations, the domestic and global economy, public confidence, civil liberties, or public health and the safety of the American people.”

A Russian cyber attack on communications or IT critical infrastructure, particularly in the context of a national emergency, would fall under this classification.

In the event of such an attack, the United States would draw together the National Cyber Response Group, which would lead the defensive response in support of
the National Security Council. The Secretary of Defense and the directors of the Intelligence Community agencies would manage incoming cyber threats, and any movement that would require an active military response. Were the telecommunications nodes of the National Security and Emergency Preparedness sector to fail, the National Coordinating Center for Communications (NCC) would be responsible for restoring those capabilities. Additionally, as part of the mandate of PPD-41, if an operation with clear attribution were to occur, the Cyber Response Group would then call upon a cadre of qualified and trained cyber personnel to mitigate and respond to the cyber incident. Theoretically, these participants would have been training together in war games and practice sessions prior to the Russian intrusion.

**U.S. STRATEGIC RESPONSES**

After mitigating the immediate effects of a significant cyber incident, the United States would consider its preponderance of strategic and tactical responses to direct toward Russia. The United States could choose to respond by non-military means, including indictment, diplomacy, or sanctions. As a lower-level military and intelligence strategy, the United States could then choose to respond with counter-surveillance intelligence operations, a non-attributable cyber or conventional attack, or an attributable cyber or conventional attack. These operations could target Russia’s military, civilian, or critical infrastructure systems. In acknowledgement of NATO’s classification of cyberspace as the fifth operational domain, it is likely that if the United States attributed a significant cyber incident on its soil to Russia, it would respond in an aggressive cyber manner. Although it is also possible that the United States would respond with purely conventional military operations, the potential escalation of this suggests that the United States would prefer to solely employ cyber operations in its response.

**LOW-LEVEL ATTRIBUTABLE CYBER INTRUSION**

The United States could respond with a low-level cyber intrusion, falling across a spectrum of cyber incidents that could not be classified as a major attack. This intrusion could appear from what has been dubbed “loud cyber weapons,” or tools that can definitively be traced back to the U.S. military. The military would send these weapons, embedded with encrypted codes, into Russian networks. The United States would then publicly provide the encryption key to claim responsibility. This intention of causing attributable damage represents a key paradigm shift in U.S. military strategy, one in which the attribution is a key aspect of a successful operation, and the publication of the attribution is vital for deterrent strategy.

The United States could also conduct simpler cyber intrusions against Russia’s network, including defacements of government websites, disruptions of Internet services, interferences and disablements of communications, or the dissemination of propaganda. Following the hack of the DNC, senior government officials discussed options for counter-cyber attacks on the Russian Federal Security Service.
The United States could use similar cyber operations to directly attack Russian military targets, which include shutting off the power at a nuclear facility or an airfield, causing serious casualties and triggering a notable escalatory threshold. Of note, many Russian industrial networks run on Windows XP, or equitable older systems, while remaining connected to the Internet. Not only are these systems extremely vulnerable to attack, but the United States has already demonstrated its ability to break into these systems. In November 2016, the United States reportedly penetrated Russian military systems and left behind malware, to be activated in the case of Russian interference of U.S. elections. This demonstrated both confidence in the success of the malware implant, and political willingness to trigger a consequential conflict.

STRATEGIC CONSIDERATIONS FOR U.S. DECISIONS

In response to a Russian cyber attack, the United State’s strategic responses would stem from its classification of the response as non-significant, significant, or an act of war. Testifying in July 2016 before the House Subcommittee on Information Technology and National Security, State Department Cyber Coordinator Chris Painter said the United States would respond to incidents on a case-by-case basis, adding that, “it could be through cyber means. It could be through diplomacy. It could be through indictments and law enforcement actions.”

(FSB) and the Main Intelligence Agency (GRU), including the utilization of the NSA’s TreasureMap tool, which tracks all global connections to the Internet, and could be used to place malware in targeted Russian computer systems for intelligence gathering and future cyber-assaults.

MEDIUM-LEVEL CYBER ATTACK – NO IMMEDIATE CASUALTIES

Using logic bombs, the United States could also conduct a cyber operation against military and non-military targets. By sending in these logic bombs to self-destruct within Russia’s critical infrastructure, the United States could cause serious economic and operational damage. It is likely these logic bombs are fairly well-developed; back in 2014, U.S. Cyber Command offered a $460 million contract to develop a “computer code capable of killing adversaries.”

HIGH-LEVEL CYBER ATTACK – POSSIBLE CASUALTIES

By using logic bombs or other cyber intrusion methods, the United States could attack Russian critical infrastructure in a more serious manner, with a larger potential for loss of human life or safety. These attacks could include hacking into a dam located above a populated area or disabling air traffic control services. These options, particularly if they are easily attributable, have the potential to escalate quickly.

MILITARY-LEVEL CYBER ATTACK – ESCALATORY

The United States could use similar cyber operations to directly attack Russian military targets, which include shutting off the power at a nuclear facility or an airfield, causing serious casualties and triggering a notable escalatory threshold. Of note, many Russian industrial networks run on Windows XP, or equitable older systems, while remaining connected to the Internet. Not only are these systems extremely vulnerable to attack, but the United States has already demonstrated its ability to break into these systems. In November 2016, the United States reportedly penetrated Russian military systems and left behind malware, to be activated in the case of Russian interference of U.S. elections. This demonstrated both confidence in the success of the malware implant, and political willingness to trigger a consequential conflict.

STRATEGIC CONSIDERATIONS FOR U.S. DECISIONS

In response to a Russian cyber attack, the United State’s strategic responses would stem from its classification of the response as non-significant, significant, or an act of war. Testifying in July 2016 before the House Subcommittee on Information Technology and National Security, State Department Cyber Coordinator Chris Painter said the United States would respond to incidents on a case-by-case basis, adding that, “it could be through cyber means. It could be through diplomacy. It could be through indictments and law enforcement actions.”
Some of these responses would require action. Such a path would depend on actual and anticipated effects of any cyber incident, including injury, damage, and death. Painter testified that, “cyber activities may in certain circumstances constitute an armed attack that triggers our inherent right to self-defense as recognized by Article 51 of the U.N. Charter.” The United States could also justifiably accuse a cyber-attack of infringing upon its territorial integrity or political independence, per Article 2(4) of the Charter.

Recent political precedents suggest that the United States would be hesitant to invoke Article 51, even if a Russian cyber attack resulted in nominal deaths, injury, or damage. Instead, it would limit its declarations and label the attack a “significant cyber incident,” invoking the full support of the U.S. military while avoiding overescalation. As well, even though NATO justified military responses within cyberspace, the lack of precedent or norms mean that the United States would actually have more creative license in responding to Russia if it were to use cyber means, that could or could not result in conventional consequences.

The United States would have to choose between a hidden or obvious counter-cyber attack. The above tactical considerations demonstrated that a hidden, non-attributable cyber attack would not fall within the Department of Defense’s deterrence strategy, and would thus be discarded as a strategic option. Following North Korea’s reported hack into Sony Pictures in 2014, the United States did not publicly respond with a cyber operation, and it was “unclear how the United States may have retaliated against the North in secret, if it even did so.” This, along with public and mild economic sanctions, now seems ineffective.

Circumstances could arise that would leave the United States with the opportunity to perform an immediately observable cyber attack (using a “loud cyber weapon”) or a preparatory attack (such as a logic bomb), and could either target a Russian military or civilian infrastructure. Similarly to Russia, the United States would also likely avoid directly targeting a military structure, to avoid escalation and a possible world war. Thus, the United States would most likely choose to deploy a cyber weapon against critical Russian infrastructure, resulting in conventional consequences. Even considered a medium-level choice in terms of escalatory possibilities, this strategic decision would have to take into account the global ramifications of an attributable cyber-to-conventional attack. General Keith Alexander testified before Congress in 2016 that attribution and response via offensive cyber capabilities must only occur if the actor is prepared to use them immediately.

**STRATEGIC RAMIFICATIONS OF RUSSIAN CYBER ATTACK AND U.S. COUNTER-ATTACK**

Although the above outlines the need for a U.S. counter-cyber attack, such a response would have drastic normative implications. Even though President Obama said in September 2016 that, “we’re moving into an era here where a number of countries...”
These attacks are costly. According to RAND, first party losses, or those incurred as a direct result of the incident (investigations, customer support, notification), and third party losses (lost revenue and market valuation) as a result of cyber incidents cost the world more than $8.5 billion annually. Between 2004 and 2015, the study found that the U.S. government faced roughly 1,300 cyber incidents.

However, the more pressing costs are those relating to deterrence. Long-term, a less reputable U.S. defense system and a lack of confidence in U.S. digital infrastructure would be damaging both economically and politically, and invite further attacks from state and non-state actors. Although cyber attacks are increasingly considered common, and businesses register thousands of penetrations each year, the world has yet to see a cyber-to-conventional attack that would trigger a significant response. Thus, the United States would have to consider the strategic implications of setting that norm.

This is not to say that the Russian attack on the U.S. electoral system, nor any potential attack on critical infrastructure, would be the first time the United States had to worry about cyber intrusions into its government systems. Even back in 1984, President Ronald Reagan saw the potential for intrusions, and signed the first Presidential Directive on computer security. The United States knew that someday, foreign entities could hack into U.S. military systems because they were already hacking into foreign systems themselves. As of 2016, more than twenty countries have offensive and defensive cyber units in their militaries, including Iran, Syria, and North Korea. The United States has been conducting counter-surveillance, intelligence, and intrusive operations against these adversaries for decades.

However, until now, the effects of these cyber battles have been limited. While militaries have registered each other’s intrusions and responded, and corporate entities have registered ongoing hacks into their systems, there has yet to be a big, public, conventional result from a cyber operation. Thus, even if Russia were to blatantly and publicly cross the normative threshold that most militaries hold themselves accountable to, the United States would be cautious about an overly zealous response, for fear of escalation.

Still, fear of escalation should not preclude U.S. response, particularly if the significant Russian attack is, in fact, significantly harmful. Although a cyber attack on U.S. infrastructure would fall under the purview of national defense, it is important to consider the economic and political consequences of such an attack, regardless of the U.S. response or any future escalation.

These attacks are costly. According to RAND, first party losses, or those incurred as a direct result of the incident (investigations, customer support, notification), and third party losses (lost revenue and market valuation) as a result of cyber incidents cost the world more than $8.5 billion annually. Between 2004 and 2015, the study found that the U.S. government faced roughly 1,300 cyber incidents.

However, the more pressing costs are those relating to deterrence. Long-term, a less reputable U.S. defense system and a lack of confidence in U.S. digital infrastructure would be damaging both economically and politically, and invite further attacks from state and non-state actors. Although cyber attacks are increasingly considered common, and businesses register thousands of penetrations each year, the world has yet to see a cyber-to-conventional attack that would trigger a significant response. Thus, the United States would have to consider the strategic implications of setting that norm.
Nicole Softness is a graduate student at Columbia University’s School of International and Public Affairs, studying International Security & Cyber Policy. Her research focuses on the intersection of counterterrorism and social media, succeeding an undergraduate thesis on al Qaeda’s messaging strategies. She is currently the Research Assistant for Columbia’s Initiative on the Future of Cyber Risk.


14. Weedon. p. 73.

15. There are a number of reasons Russia would likely avoid a cyber attack directed at the following critical infrastructure sectors:

- Chemical: likely to cause panic and escalate into war
- Defense: likely to escalate or qualify as an act of war
- Emergency Systems: likely to escalate, qualify as an act of war, or cause loss of life
- Healthcare and Public Health: likely to incite national panic and resulting military actions
- Nudiear: likely to escalate or qualify as an act of war
- Dams: too involved with energy, likely to incite
- Transportation: could cause too many accidents and loss of life
- Government Facilities: direct act of war
- Energy: too many global industries dependent on energy or overlap with health concerns
- Waste: biohazards could cause loss of life
- Financial: would incite U.S. economic allies or could damage Russian alliances
Food & Agriculture: too many global actors dependent on U.S. resources

Critical Manufacturing: facilities partners all over the world or too interdependent with


Lipton, Sanger, and Shane, The Perfect Weapon.


21. NTIA. p. 3.

22. NTIA. p. 3.

23. NTIA. p. 3.


29. Information Technology Sector.


44. Testimony of Christopher M. E. Painter. 


44. Testimony of Christopher M. E. Painter. 


52. Romanosky.