COUNCIL *on* FOREIGN RELATIONS

CYBER BRIEF

Developing a Proportionate Response to a Cyber Incident

Tobias Feakin
August 2015

This Cyber Brief is part of the Digital and Cyberspace Policy program.

As offensive cyber activity becomes more prevalent, policymakers will be challenged to develop proportionate responses to disruptive or destructive attacks. Already, there has been significant pressure to "do something" in light of the allegedly state-sponsored attacks on Sony Pictures Entertainment and the Sands Casino. But finding a timely, proportionate, legal, and discriminatory response is complicated by the difficulty in assessing the damage to national interests and the frequent use of proxies. Perpetrators have plausible deniability, frustrating efforts to assign responsibility. Past experience suggests that most policy responses have been ad hoc.

In determining the appropriate response to a state-sponsored cyber incident policymakers will need to consider three variables: the intelligence community's confidence in its attribution of responsibility, the impact of the incident, and the levers of national power at a state's disposal.

While these variables will help guide responses to a disruptive or destructive cyberattack, policymakers will also need to take two steps before an incident occurs. First, policymakers will need to work with the private sector to determine the effect of an incident on their operations. Second, governments need to develop a menu of preplanned response options and assess the potential impact of any response on political, economic, intelligence, and military interests.

BACKGROUND: CYBER INCIDENTS AND UNCERTAINTY

Even as the number of highly disruptive and destructive cyberattacks grows, governments remain unprepared to respond adequately. In other national security areas, policy responses to state-sponsored activity are well established. For example, a country can expel diplomats in response to a spying scandal, issue a demarche if a country considers its sovereignty to have been violated, and use force in response to an armed attack. Clear and established policy responses such as these do not yet exist for cyberattacks for two reasons. First, assessing the damage caused by a cyber incident is difficult. It can take weeks, if not months, for computer forensic experts to accurately and conclusively ascertain the extent of the damage done to an organization's computer networks. For example, it took roughly two weeks for Saudi authorities to understand the extent of the damage of the Shamoon incident, which erased data on thirty thousand of Saudi Aramco's computers. Although this may be quick by computer forensics standards, a military can conduct a damage assessment from a non-cyber incident in as little as a few hours.

Second, attributing cyber incidents to their sponsor remains a significant challenge. Masking the true origins of a cyber incident is easy—states often use proxies or compromised computers in other jurisdictions to hide their tracks. For example, a group calling itself the Cyber Caliphate claimed responsibility for taking French television station TV5 Monde off the air with a cyberattack in April 2015, and used the television station's social media accounts to post content in support of the self-proclaimed Islamic State. Two months later French media reported that Russian state-sponsored actors, not pro–Islamic State groups, were likely behind the incident. Even when attribution is possible, it is not guaranteed that domestic or foreign audiences will believe the claim unless officials reveal potentially classified methods used to determine the identity of the perpetrator, damaging intelligence assets. Under pressure, responses are likely to be made quickly with incomplete evidence and attract a high degree of public skepticism. This creates clear risks for policymakers. Quick damage assessments could lead to an overestimation

of the impact of an incident, causing a state to respond disproportionately. Misattributing an incident could cause a response to be directed at the wrong target, creating a diplomatic crisis.

DEVELOPING A PROPORTIONATE RESPONSE

Policymakers should consider three variables before developing a response. First, they should understand the level of confidence that their intelligence agencies have in attributing the incident. Although there have been great strides in intelligence agencies' ability to attribute malicious activity, digital forensics is not perfect. The degree of attributional certainty will have a direct impact on the action taken. For example, if the level of attribution is low, policymakers will be limited in their choice of response even if the severity of the attack is high. They may choose a less valuable retaliatory target to limit the odds of escalation and international criticism. There may be also instances where there is so little evidence for the source of the attack that the victim may choose not to respond.

Second, policymakers should assess the cyber incident's effects on physical infrastructure, society, the economy, and national interests. Questions include: What was the physical damage caused by the affected systems, and was there any impact to critical infrastructure? What type of essential services are affected? Has the incident caused a significant loss of confidence in the economy? What was the incident's impact on national security and the country's reputation?

Third, policymakers should consider the range of diplomatic, economic, and military responses at their disposal, from a quiet diplomatic rebuke to a military strike. Responses need not be limited to cyberspace—nothing bars a state from using other channels, though each carries its own risks.

Cyber responses can be taken in addition to diplomatic, economic, and military activity. However, they would most often be delivered covertly and could be difficult to develop quickly unless a government had prepared capability against a specific target, likely involving prior cyber espionage, an unparalleled understanding of a target's vulnerabilities, and a custom exploit kit at its disposal. As an example, Stuxnet reportedly took years to develop and deploy. An overt cyber response can be unappealing as states may lose the ability to launch similar responses against other targets. Although states may outsource their responses to a proxy, doing so could limit their control over the response and lead to escalatory activity. Therefore, policymakers are likely to concentrate on other levers of power, alongside whatever they may do covertly.

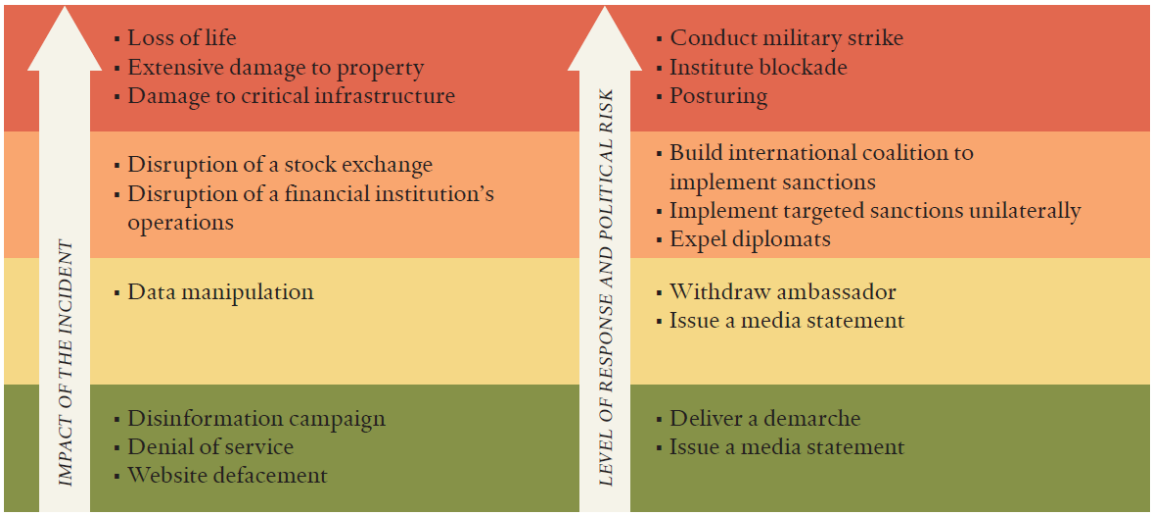
RECOMMENDATIONS

Given the likely pressure governments will feel to respond to significant cyberattacks, policymakers need to develop a response framework before a disruptive or destructive cyber incident occurs. Although each response will be case-specific, a framework will enable policymakers to quickly consider their options.

Figure 1 represents a possible framework that policymakers can build on. Combining incident impact, policy options, and proportionality, it outlines the different levers of state power that can be applied in response to escalating levels of cyber incident. It plots the effects of a cyber incident, with website defacement at one end of the scale and loss of life at the opposite end. This is plotted against

the level of response, ranging from media statements to military responses. Across the response spectrum there will be inherent political and legal risks associated with each decision, and risks increase as the level of the response increases. The proposed responses are applicable to state-sponsored activity. For disruptive or destructive activity caused by individuals, criminal networks, or others without state-backing, law enforcement responses are more appropriate.

FIGURE 1. POLICY RESPONSES TO ESCALATING STATE-SPONSORED CYBER INCIDENTS.



As with other areas of international relations, proportionality emerges through state practice—the expulsion of diplomats in response to a mild violation of sovereignty is perceived as proportionate only because states have been doing it for decades. When one country levies economic sanctions, the sanctioned country often responds in kind—Russia responded to U.S. sanctions over its annexation of Crimea with sanctions of its own. This same logic applies to cyberspace. While there may be pressure to respond disproportionally to deter future attacks, international law requires that states only take forcible measures that are necessary and proportionate to successfully repel or defeat a disruptive or destructive cyberattack, limiting the "scale, scope, duration and intensity" of any action a victim state may take. Furthermore, responding proportionally may make it easier to build the international coalitions necessary to isolate and punish the attacker as well as limit the likelihood of escalation.

If a country is the victim of a state-sponsored website defacement, a public denouncement is likely the most appropriate response. Moving up the scale, any activity that begins to manipulate or destroy data would potentially require diplomatic action, such as a demarche in low-impact cases or the expulsion of diplomats if the incident affects the victim's economy. Once the economy is adversely affected, a range of economic responses can be used in coordination with diplomatic pressure, from freezing individuals' financial transactions within the sponsoring state to levying international sanctions. Should an incident cause physical damage, a policymaker could consider a military option as an appropriate and proportional response, from military posturing to an attack depending on the incident's severity. All of these options can be complemented with cyber or covert action, which will also need to be proportionate to the damage caused by the incident.

Each state can begin developing its own policy response framework by first working with the private sector, particularly in critical infrastructure. Critical infrastructure is a priority for attackers, making it important for infrastructure operators to be involved in the development of a response framework. They are in a good position to advise government on incidents that would affect their operations and how severe an incident would need to be before a response is required.

Second, policymakers should clearly understand the costs associated with each response in the framework. Each response will have an impact on a country's diplomatic relations, reputation, and military and intelligence operations. These effects need to be understood before a response is chosen. Assessing options will require input from relevant government agencies, as well as critical infrastructure operators, whose operations could be affected by a response.

Cyber incidents provide governments with a highly complex set of decisions to make, from understanding the severity of the incident to assessing appropriate responses to take, while continually evaluating the risks involved in taking certain courses of action. The framework, while deliberately simplified, provides a rudimentary model for framing the potential responses to a state-sponsored incident before one occurs. This should give policymakers a starting point from which to make their own assessments on courses of action to take during a time of crisis.

About the Author

Tobias Feakin is a senior analyst and director of the International Cyber Policy Centre at the Australian Strategic Policy Institute. In 2014 he was appointed by the Australian Prime Minister to an expert panel to assist the government with its Cyber Security Review. He is an Oxford Martin associate for Cyber Security at the University of Oxford. He was previously a senior research fellow and director of the National Security and Resilience department at the Royal United Services Institute (RUSI) in London, where he is still an associate fellow. He has lectured at the University of Cambridge, University of Bradford, Joint Services Command and Staff College, and the NATO Defence College in Rome, and regularly appears on the BBC, ABC, Channel 4 (UK), NBC, Al Jazeera, and Sky News.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR carries out its mission by maintaining a diverse membership, with special programs to promote interest and develop expertise in the next generation of foreign policy leaders; convening meetings at its headquarters in New York and in Washington, DC, and other cities where senior government officials, members of Congress, global leaders, and prominent thinkers come together with CFR members to discuss and debate major international issues; supporting a Studies Program that fosters independent research, enabling CFR scholars to produce articles, reports, and books and hold roundtables that analyze foreign policy issues and make concrete policy recommendations; publishing *Foreign Affairs*, the preeminent journal on international affairs and U.S. foreign policy; sponsoring Independent Task Forces that produce reports with both findings and policy prescriptions on the most important foreign policy topics; and providing up-to-date information and analysis about world events and American foreign policy on its website, CFR.org.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.

The Digital and Cyberspace Policy program addresses one of the twenty-first century's most pressing challenges: keeping the global Internet open and secure in the face of unprecedented threats. Through briefings, reports, and the *Net Politics* blog, the program's fellows produce timely analysis on the most important issues in cyberspace. Cyber Briefs are short memos that offer concrete recommendations on cybersecurity, Internet governance, online privacy, and the trade of digital goods and services.

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.