ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Jason Healey

CYBER STATECRAFT INITIATIVE

Beyond Attribution: Seeking National Responsibility for Cyber Attacks

For more than two decades, cyber defenders, intelligence analysts, and policymakers have struggled to determine the source of the most damaging attacks. This “attribution problem” will only become more critical as we move into a new era of cyber conflict with even more attacks ignored, encouraged, supported, or conducted by national governments.

Analysts often fall into the trap of “attribution fixation,” the belief that they cannot assess which organization or nation was behind an attack until technical forensics discovers the identity of the attacking machines. Because the Internet enables anonymity more than security, this bottom-up process rarely succeeds.

Fortunately, there is another option.

For national security policymakers, knowing “who is to blame?” can be more important than “who did it?” Moreover, attribution becomes far more tractable when approached as a top-down policy issue with nations held responsible for major attacks originating from their territory or conducted by their citizens.

Meeting the needs of policymakers must be the end goal of attribution, not a byproduct. So, in addition to making the case for national responsibility for cyber attacks, this paper proposes a spectrum of state responsibility to more directly tie the goals of attribution to the needs of policymakers.[1]

What Stones Teach Us

In 1999, NATO mistakenly bombed the Chinese embassy in Belgrade during an airstrike to compel Yugoslavia to withdraw forces from Kosovo. Furious Chinese targeted the United States embassy in Beijing (among other embassies and consulates), smashing windows with stones and tearing up nearby roads to use as more projectiles. Yet the US intelligence community and National Security Council staff did not spend much time watching video to backtrack trajectories in order to identify the individual stone throwers. There was no need to indulge in litho-ballistic forensics because exact attribution was not an important input for decision-makers.

About the Cyber Statecraft Initiative

The Atlantic Council’s Cyber Statecraft Initiative helps foster international cooperation and understanding of new forms of cooperation and conflict in cyberspace through global engagement and thought leadership.

This is an edited version of a paper that first appeared in the *Brown Journal of World Affairs*.

This paper was made possible by generous support by Saab North America, Inc.

Policymakers knew that to reduce these Chinese government-encouraged stone-throwing attacks, it needed to coerce, engage, or assuage the Chinese government. Chinese police controlled the area but permitted the stone-throwing; many protesters were transported by bus from state-run universities in organized processions; and, to cap it off, then-Vice President Hu Jintao made state support explicit in a televised statement. Knowing the identity of the stone throwers would have provided thousands of data points, but none that were relevant to decision-making.

[1] In this paper, “attack” is used in its technical meaning, referencing a malicious cyber incident. The term here does not imply that the incident necessarily rises to the level of “armed attack.”

Jason Healey is the Director of the Cyber Statecraft Initiative at the Atlantic Council of the United States. You can follow his comments on cyber issues on **Twitter at @Jason_Healey**.

Eight years later, in an environment of emotional Russian nationalism, cyber attacks inundated Estonia. Many of the attacks were traced to Russia, followed “instructions provided on Russian-language Internet forums and websites,” and were supported by comments from senior Russian politicians. As with the Chinese government’s blind-eye for stone throwing, the Russian government refused to investigate or stop the attacks, leaving Russian police on the sidelines.

Despite these direct parallels between the Chinese and Russian governments’ actions, too many analysts felt attribution fixation: the compulsion to comprehensively backtrack the trajectory of the cyber-stones. Just as during the China protests, the source of each individual attack simply was not relevant to the most important decisions.

In the case of Estonia, these analysts determined the attacks traced back to 178 countries, including the United States. But so what? This mass of useless forensic facts resulted in only one prosecution and worse, served to muddy the obvious truth: the attacks were supported or encouraged by the Russian government and that to make the attacks stop, Western decision-makers needed to engage Moscow.

This was self-evident when the projectiles were stones, but became somehow mystifying when the projectiles were electrons. Once reduced to this level, it is hopefully easier to recognize that stopping a state-encouraged attack need not depend on tracing every attack, but holding that government responsible. But what does “responsibility” really mean in this context? To ask the question more broadly, in what ways is a nation responsible for cyber attacks from its territory or conducted by its citizens?

The Spectrum of State Responsibility

The spectrum of state responsibility is a tool to help analysts with imperfect knowledge assign responsibility for a particular attack, or campaign of attacks, with more precision and transparency. This spectrum assigns ten categories, each marked by a different degree of responsibility, based on whether a nation ignores, abets, or conducts an attack. The spectrum starts from a very passive responsibility—a nation having insecure systems that lead to an attack—up to very active responsibility—a national government actually planning and executing an attack.

The Spectrum of State Responsibility

1. **State-prohibited.** The national government will help stop the third-party attack
2. **State-prohibited-but-inadequate.** The national government is cooperative but unable to stop the third-party attack
3. **State-ignored.** The national government knows about the third-party attacks but is unwilling to take any official action
4. **State-encouraged.** Third parties control and conduct the attack, but the national government encourages them as a matter of policy
5. **State-shaped.** Third parties control and conduct the attack, but the state provides some support
6. **State-coordinated.** The national government coordinates third-party attackers such as by “suggesting” operational details
7. **State-ordered.** The national government directs third-party proxies to conduct the attack on its behalf
8. **State-rogue-conducted.** Out-of-control elements of cyber forces of the national government conduct the attack
9. **State-executed.** The national government conducts the attack using cyber forces under their direct control
10. **State-integrated.** The national government attacks using integrated third-party proxies and government cyber forces

Countries that fall into the first two categories have only very passive responsibility since they will, at the least, attempt to cooperate with the nation under attack.

State-prohibited. The national government will help stop the third-party attack, which may originate from its territory or merely be transiting through its networks. This responsibility is the most passive on the scale: though the government is cooperating, it still has some small share of responsibility for the insecure systems involved in the attack. In reality, nations cannot ensure the proper behavior of the tens or hundreds of millions of computers in their borders at all times.

State-prohibited-but-inadequate. The national government is cooperative and would stop the third-party attack but is unable to do so. The country might lack the proper laws, procedures, technical tools, or political will to use them. Though the nation could itself be a victim, it bears some passive responsibility for the attack, both for being unable to stop it and for having insecure systems in the first place.

In the following four categories, in contrast to the previous two, the nation is actively ignoring or abetting attacks:

State-ignored. The national government knows about the third-party attacks but, as a matter of policy, is unwilling to take any official action. A government may even agree with the goals and results of the attackers and tip them off to avoid being detected.

State-encouraged. Third parties control and conduct the attack, but the national government encourages them to continue as a matter of policy. This encouragement could include editorials in state-run press or leadership publicly agreeing with the goals of the attacks; members of government cyber offensive or intelligence organizations may be encouraged to undertake supportive recreational hacking while off duty. The nation is unlikely to be cooperative in any investigation and is likely to tip off the attackers.

State-shaped. Third parties control and conduct the attack, but the state provides some support, such as informal coordination between like-minded individuals in the government and the attacking group. To further their policy while retaining plausible deniability, the government may encourage members of their cyber forces to undertake "recreational hacking" while off duty.

State-coordinated. The national government coordinates the third-party attackers—usually out of public view—by "suggesting" targets, timing, or other operational details. The government may also provide technical or tactical assistance. Similar to state-shaped attacks, the government may encourage its cyber forces to engage in recreational hacking during off hours.

In the final four categories, the state, far from ignoring or encouraging attacks, has a much more direct hand in them, either ordering attacks or conducting them itself.

State-ordered. The national government, as a matter of policy, directs third-party proxies to conduct the attack on its behalf. This is as "state-sponsored" as an attack can be, without direct attack from government cyber forces. Any attackers that are under state control could be considered to be de facto agents of the state under international law.[2]

State-rogue-conducted. Elements of cyber forces of the national government conduct the attack. In this case, however, they carry out attacks without the knowledge, or approval, of the national leadership, which may act to stop the attacks should they learn of them. For example, local units or junior officers could be taking the initiative to counterattack out of the senior officers' sight. More worrisome, this category could include sophisticated and persistent attacks from large bureaucracies conducting attacks that are at odds with the national leadership. Based on current precedence, a state could likely be held responsible by international courts for such rogue attacks.

State-executed. The national government, as a matter of policy, directly controls and conducts the attack using its own cyber forces.

State-integrated. The national government integrates third-party attackers and government cyber forces, with common command and control. Orders and coordination may be formal or informal, but the government is in control of selecting targets, timing, and tempo. The attackers are de facto agents of the state.

The spectrum can be used both to describe individual attacks or a campaign of related attacks, and is meant to be both for the operational cyber defenders ("*General, this attack against us is probably* state-ordered. *If we ask that nation for cooperation, they will not help us, and we will tip our hand.*") and the policy community ("*The policy of our nation is to hold nations accountable for any state-ordered attacks as if those attacks were coming from the uniformed military services. You can't hide behind proxies.*").

Any cyber campaign is likely to fit into one of these ten categories, depending on the mix of the three ways nations are responsible for cyber attacks: they can ignore, abet, or conduct attacks.

[2] Being "de facto agents of the state" is a key element in legal analysis of responsibility for terrorism. A fair summary of existing international legal precedents is that "states must direct or control—rather than simply support, encourage, or even condone—the private actor." From Derek Jinks, "State Responsibility for the Acts of Private Armed Groups," *Chicago Journal of International Law, Vol. 4* (2004).

"I'm shocked, shocked to find stone throwing!" Nations are held responsible for *ignoring* attacks by refusing to acknowledge the attack. (For example, by sidestepping requests to investigate, by being unable to stop or investigate attacks coming from its cyber territory, or by having an insecure national information infrastructure.) Fostering an environment in which attacks can occur is generally a passive way for a nation to accumulate responsibility, compared to abetting and conducting (see below).

"Comrade, please throw these stones at that window." Nations are held responsible for *abetting* attacks by directly or indirectly encouraging or supporting the attack. Encouragement ranges from the relatively benign (editorials egging on the attacks) to the hostile (giving informal targeting advice or even cash).

"Release the stones!" Nations are held responsible for *conducting* attacks either by executing a decision made by the national government, or as a result of attacks carried out by elements of their government without official approval. This is the most active responsibility a nation can have.

"Cyber Somalia" and National Responsibility for Cyber Attacks

In cyberspace, states do not and cannot have the same level of control as they do over their airspace or sovereign waters. They will, however, have to take more responsibility to "shrink the sanctuaries" from where criminals act with impunity.

Unfortunately, the international community places few expectations on nations to reduce attacks originating from or routing through systems in their sovereign territory. This situation is similar to the low international expectations of a range of "ungoverned spaces" across the world. For example, the Somali government cannot police its own territory, so the international community does not expect it to patrol its offshore waters. Accordingly, the United States, France, Japan, China, and other nations have stationed their own fleets in the area (with permission to chase pirates into Somali territorial waters) while shipping companies buy more insurance and post mercenaries on their ships.

Unfortunately, the international community generally treats cyber attacks as if every country were Somalia: helpless to restrain attacks from its territory or mitigate their downstream impacts. This, however, is not the only model for dealing with piracy, nor does it have to be the only model for cyber attacks. Piracy in the Strait of Malacca was reduced by 95 percent when Singapore, Malaysia, and Indonesia recognized their dependence on trade and international trust and, setting aside regional differences, cooperatively asserted their national power through patrolling, information sharing, and other military collaboration, according to *TIME* magazine. In an unconscious parallel to cyber security, one observer summarized that, "It dawned on the states that piracy is transnational and nothing that could be handled by one nation alone […]. The sea doesn't respect borders."

> *Unfortunately, the international community generally treats cyber attacks as if every country were Somalia: helpless to restrain attacks from its territory or mitigate their downstream impacts.*

Under international pressure, most nations could likewise reduce attacks from their territory of cyberspace through several well-established steps, including prioritizing security hiring, policies, and projects; pushing for improved security for computers in homes, universities, businesses, and governments; setting higher expectations for service providers to identify and stop attacks; funding and training effective incident response teams; and ensuring adequate resources for law enforcement and international cooperation. Nations that support hacking groups, for patriotic or economic reasons, should feel pressure to rein them in—indeed, the Estonian national cyber strategy calls for efforts to "achieve worldwide moral condemnation of cyber attacks that affect the functioning of society and impinge directly on people's well-being." All of these steps will establish that most nations are not as helpless as Somalia, and should meet expectations to secure their cyberspace, cooperating with others as necessary.

Saying that nations should be "responsible" for their part of cyberspace is related to, but not quite the same thing as, saying nations should have "sovereignty" over cyberspace. Sovereignty is a well-defined legal concept, and there is a growing body of practice and scholarly articles on the application of national sovereignty in cyberspace.[3] This paper, however, is not advancing any such legal argument about sovereignty. Rather, this paper argues that as a policy (not legal) matter, nations can and should hold one another responsible to stop attacks and clean the cyber environment.

While it is not official US policy to hold nations responsible for attacks from their territory or conducted by their citizens, the International Strategy for Cyberspace from the White House laid out what may be its future foundations:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country [and] recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners.
>
> We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.

Moreover, national responsibility falls in line with existing international agreements. As summarized by David Graham, the United Nations General Assembly "has called upon states to […] prevent their territories from being used as safe havens [and] cooperate in the investigation and prosecution of international cyber attacks." There has even been some existing state practice which will be the focus of the next section.

National Responsibility in Practice

The most important example of national responsibility for cyber attacks came in early 2010 after intrusions into the networks of Google (a US company) became public and were loosely traced back to China. Soon after, the US Department of State issued a *démarche* to the Chinese government and Secretary of State Hillary Clinton set the US government's expectations: "We look to Chinese authorities to conduct a thorough investigation of the cyber intrusions that led Google to make this announcement […] We also look for that investigation and its results to be transparent." Secretary Clinton was not making any specific sovereignty claims for either the United States or China, but was instead setting the policy that China was responsible in settling this potential dispute between countries.

Similarly in Beijing in 2011, according to press, a senior State Department official "raised the case of a hacked US political site directly with the Chinese Ministry of Foreign Affairs" while in 2007, German Chancellor Angela Merkel complained to Hu Jintao about Chinese intrusions into her own computer.

These cases clearly show that policymakers already are thinking in terms of national responsibility, not attribution. "Make this stop" is the common theme, not "who did it," and this national responsibility approach opens up the full range of coercive options that policymakers are already familiar with.

For example, if Estonia or another US friend or ally is attacked again, the National Security Council should start by determining which head of state or government it recommends the president should call and what carrots and sticks are available. The following conversation between the president of the United States and the president of Russia is entirely a thought experiment, to show what is possible without exact attribution:

"We understand your assurance that Russia is not conducting these attacks against our treaty partner Estonia; thank you for that affirmation and your promised investigation. However, we need these attacks to stop, and we look to Russia for help.

First, I would like you and your prime minister to make clear statements that these attacks need to stop. To date, your assurances have not been as clear as what you just made to me. Second, an FBI team is assembling their gear and will be airborne tomorrow, en route to Moscow to assist your investigation. They will share all the forensic data we have collected, and expect the same. They are already in touch with your embassy here but we may need your help to ensure they get visas immediately.

I am under intense international and domestic pressure for action. Many in the public and press are not taking at face value that your government is not involved. Every official

[3] Beginning in earnest with French government pressure in 2000 against Yahoo! to prevent access in France to pro-Nazi material, a case well examined in: *Who Controls the Internet: Illusions of a Borderless World* by Jack Goldsmith and John Wu; in particular, reference the writings of Sean Kanuck ("Sovereign Discourse on Cyber Conflict" in the Texas Law Review, 2010), David Graham ("Cyber Threats and the Law of War" in the *Journal of National Security Law and Policy*, 2010), Patrick Franzese ("Sovereignty in Cyberspace" in *Air Force Law Review*, 2009). These authors all have general consensus around certain points, such as (in Franzese's words), "Many of the designers of cyberspace viewed it as an intellectual nirvana free from the constraints of the 'real' world. In reality, however, cyberspace is part of the 'real' world and thus subject to its constraints and order—in other words, subject to state sovereignty."

denial from the Russian government is matched by many more unofficial messages egging on the attacks.

Since the best way to convince these critics is for Russia to cooperate, I will continue to hold them off as long as you and I are communicating and our joint investigation is progressing. My message remains that we should accept your personal assurances, backed by real cooperation.

> *States on the receiving ends of continuing attacks must have recourse to the traditional full spectrum of coercive policies.*

However, if our dialog breaks down, the investigation meets roadblocks, or the Russian government continues to egg on the attackers, you force me to assume the worst. I'll have no choice but to believe that you have not been entirely truthful and your government is encouraging, coordinating, or even participating in these attacks. Then, I of course will have to change my message and agree that yes, we must assume the Russian government is complicit in this cyber attack on Estonia.

In this unfortunate event, I will recommend NATO immediately begin Article 4 consultations, deploy a rapid reaction team to Estonia to assist their defense and start considering thresholds for Article 5. Even if NATO ultimately does not act in this matter, the United States will be prepared to act alone to support our alliance partner. I have spoken to the commanders of our cyber forces and, on their advice, ordered them to a higher alert status. This will help us improve our own defense and speed planning to assist in the defense of our ally's cyber territory, should I so order.

This should not be a surprise, as I made clear in my cyber strategy, the United States stands by our allies, even in cyberspace. While neither you nor I want such an outcome, I am confident the American people and the international community would support limited counteractions to blunt the attacks.

I am sure some of these attacks will trace back to the United States and other countries and I pledge my government's help to stop them. May I count on you to do the same?"

This thought experiment is of course not a foolproof way to stop future Estonia-style attacks and is meant only to show what policy levers may be usable absent exact attribution. This approach displays four key advantages. First, it puts policy front and center, not as a by-product or end-product of attribution. Second, positive technical attribution does not even matter as the argument rests solely on holding a nation accountable for attacks organized by its citizens or coming from its territory. Third, it re-establishes state-to-state symmetry. Even though the attacks may be undertaken by non-state actors, this approach holds the offending government responsible. Fourth, it is rooted in national security fundamentals: one president signaling another about unacceptable behavior. By decoupling the incident from any technical jargon, the National Security Council staff and president will find it far easier to understand and engage their instincts, education, and experience.

Pitfalls of National Responsibility

Holding nations responsible for attacks in this manner offers more promise than a continuation of the current attribution fixation. It does, however, bring some problems of its own. First, like-minded nations need to join in multilateral cooperation and collective defense, advocate for better security, and establish norms (the "rules of the road") for cyber cooperation, conflict, and competition. Second, accountability will be a double-edged sword: each nation will need to lessen its own potential culpability by reducing its population of infected machines and securing its systems. If it does not, that nation could itself be held responsible for damage to nations on the receiving end of attacks from its cyber soil. The United States in particular will find itself in a difficult position: it is the country targeted by 65 percent of all denial-of-service attacks (floods of traffic that disrupt normal operations of computers or networks), the most of any country, according to cybersecurity company Symantec. The United States is also the top source for attacks, accounting for 22 percent of the global total. Essentially, United States is simultaneously both the prime victim of, and main sanctuary for, cyberattacks.

Third and most important, a push for national responsibility of cyberspace could be manipulated by nations to clamp down on an individual's right to freedom of opinion and expression "through any media and regardless of frontiers" as codified in the 1948 Universal Declaration of Human Rights. Perhaps the best example of this is the official agreement put forth by the Shanghai Cooperation Organization (SCO) comprised of China, Russia, and central Asian nations. In a 2008 declaration, the SCO expressed their worry about the "use of the dominant position in the information space to the detriment of the interest and security of other States [...] [and] dissemination of information harmful to social and political, social, and economic systems, as well as spiritual, moral, and cultural spheres of other States." These nations feel threatened by the flow of information from the United States, which is in the "dominant position in the information space." This type of information presumably includes hard news from CNN and "harmful" information from Twitter or Facebook that might cause a "moral" or "spiritual" impact such as questioning the legitimacy of the ruling party.

To help counter such efforts (as well as recent Internet crackdowns in Egypt, Tunisia, and elsewhere as part of the "Arab Spring") the United States has put "Internet freedom" at the center of both actions and public speeches. In fact, Freedom House recently ranked the United States second for respect for Internet freedom in the world, just behind Estonia. However, since the United States remains such a major source of global attacks, to improve credibility, some government resources may need to shift to reducing the number of outbound attacks.

The Australian government has tried to address this balance in their national security strategy by distinguishing *cyber security* (e.g., protecting confidentiality) from *cyber safety* (stopping cyber stalking and bullying, protecting children from pornography). Within the limits of the Universal Declaration of Human Rights, Australia is looking to intervene in the Internet and online behavior far more strongly than other countries. Australia's policy is still new, and whether making this distinction will be in the overall interest of Australia's citizens and its neighbors in cyberspace is still an open question. However, it is a conceptual move forward that is likely to be picked up by other nations.

Conclusion

To rein in attacks raging across the Internet, the international security community must focus on the needs of policymakers, which is best served by looking to the responsibility of nations. Too much time has been wasted obsessing over which particular villain pressed the *ENTER* key.

This paper accordingly introduced the spectrum of state responsibility to shift the discussion away from "attribution fixation," to national responsibility for attacks in cyberspace. The global national security community needs to shift resources from the technical attribution problem to solving the responsibility problem. This re-establishes state-to-state symmetry and enables a wider range of options open to sovereign nations: diplomatic, intelligence, military, and economic responses. Nations cannot use these levers of power against an individual stone-thrower, but can use them against the nation that abets him. For countries that are willing to cooperate to reduce the numbers of insecure systems, there should be offers of funding, training, education, and access to technology. If a nation repeatedly refuses to cooperate, states on the receiving ends of continuing attacks must have recourse to the traditional full spectrum of coercive policies, from *démarches* to sanctions in the UN Security Council, prosecution in international courts, and all the way to covert action and kinetic military force.

Cyberspace will be insecure until all nations are more responsible and restrictive of both inbound and outbound attacks. Moving from "who threw that stone?" to "who is to blame for stone throwing?" will be a crucial step to a more stable and secure cyberspace.

JANUARY 2012

The Atlantic Council is a non-partisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1101 15th Street, NW, Washington, DC 20005 (202) 463-7226
www.acus.org