Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF

Innovation on Cyber Collaboration: Leverage at Scale

MAY 2018 JASON HEALEY

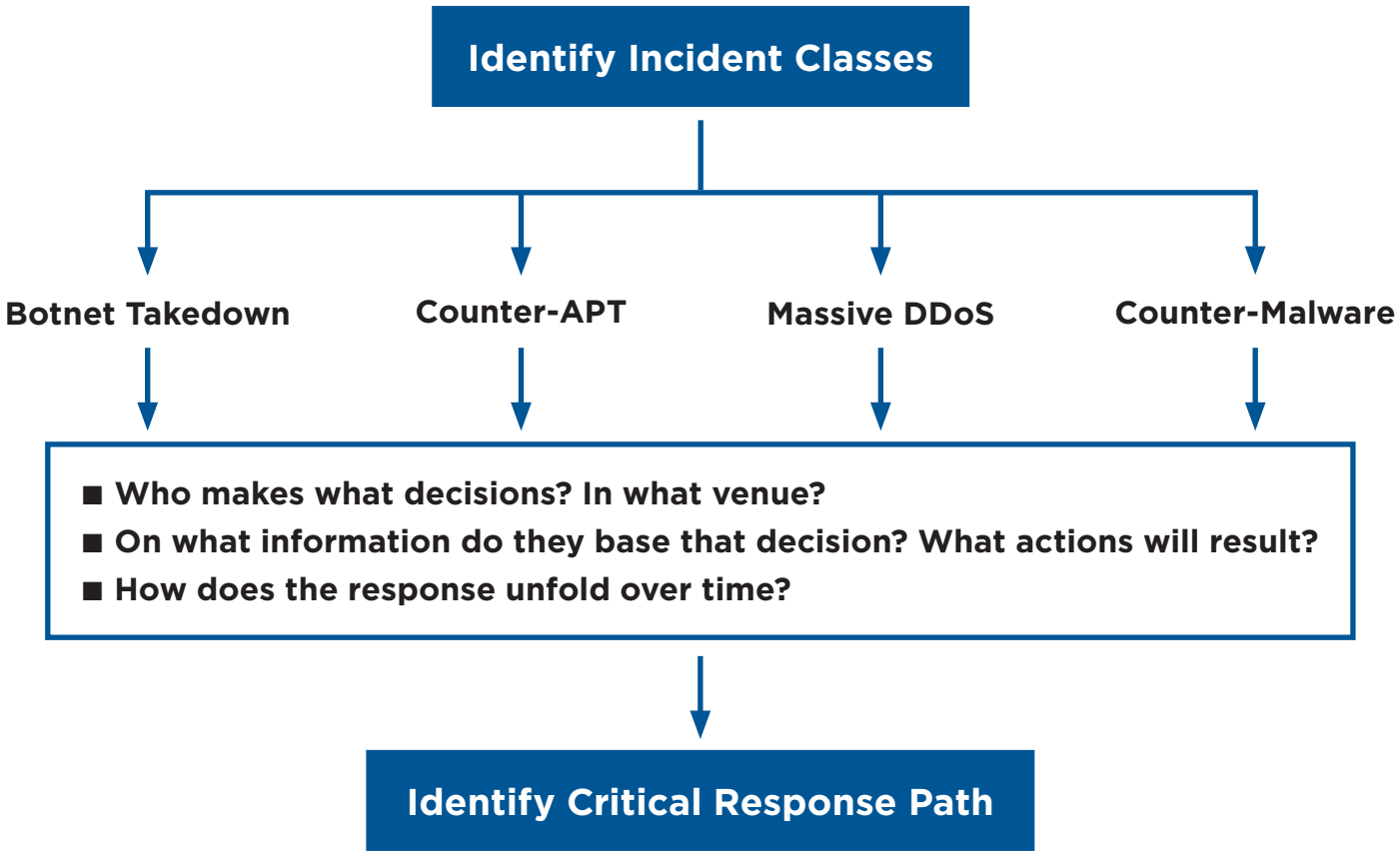
A football team can be an amazing machine for scoring touchdowns and winning football games. And any good football team must, of course, share information, from the style of opposing teams to "Hey, blitz coming, cover that guy" and "I'm open!" Yet, no coach would win football games by purposely building an information-sharing team. Yet all too often, in cybersecurity, information sharing has "become an end in itself, rather than a means to the end of actually closing vulnerabilities, stopping espionage operations, and defeating denial-of-service (DoS) attacks."[1]

For twenty-five years, national cyber strategies and policies have treated sharing as paramount.[2] The most recent important cyber legislation dealt only with sharing, and most of the key cybersecurity organizations are built around sharing. Many of these initiatives have had great success (and the author has helped run one of the key sharing organizations).

In cybersecurity, it is time to go beyond sharing and ad hoc cooperation, to collaboration at scale across borders, stakeholders, and sectors. This effort should begin with a determined study of the responses to past incidents and how to improve them, then proceed to new, action-oriented organizations to streamline response.

1 Jason Healey, *Breaking the Cyber-Sharing Logjam* (Washington, DC: Atlantic Council, 2015), http://www.atlanticcouncil.org/images/publications/AC_BreakingCyber-SharingLogjam_WEB.pdf.

2 White House, "Presidential Decision Directive/NSC-63," May 22, 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm; Department of Homeland Security, *The National Strategy to Secure Cyberspace* (Washington, DC: DHS, 2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf; White House, "Executive Order 13636 of February 12, 2013, Improving Critical Infrastructure Cybersecurity," https://www.gpo.gov/fdsys/granule/CFR-2014-title3-vol1/CFR-2014-title3-vol1-eo13636.



Determine How We Have Responded to Past Incidents

As the NY Cyber Task Force recently argued, "Although global responses like the takedown of massive botnets show that sharing and cooperation can make a tremendous difference, such collaborations are still extremely time and resource intensive."[3] That report pushed the concept of "leverage"—those actions giving defenders the greatest advantage, at the greatest scale and lowest cost—and found that operational innovations, such as collaboration and new organizational models, were overlooked sources of leverage.

There has not been any disciplined attempt to study the major incident responses of the past: who took what decision, based on what information, leading to what action, and with what ultimate result? How can defenders know what information needs to be shared, or how best to improve response? The first step to building a dream team is a disciplined process to understand and improve response for each kind of **incident class** (such as botnet takedown, counter-APT (advanced persistent threats), massive disrupted denial-of-service (DDoS) attacks, counter-malware, etc.).

The Department of Homeland Security (DHS) should, accordingly, fund a project with a think tank or Federally Funded Research and Development Center (FFRDC) to fully map the critical response path for two to four exemplars of each major incident class. These **response-path maps** for each incident type should not simply consist of a root-cause analysis, after-action report, or incident repository—as useful as those would

3 New York Cyber Task Force, *Building a Defensible Cyberspace* (New York: Columbia University School of International and Public Affairs, 2017), https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

be.[4] Each response-path map should be a detailed chart focused on the systemwide response actions and decisions that led to the resolution of the incident. Who made which decisions, and in what venue? On what information did they base that decision, and what actions resulted? If the campaign lasted for months, the maps must reflect how the response unfolded over time. This analysis should also examine if these are indeed the most important incident classes, and the amount of overlap between incident classes.

The right people could do a good-enough job with a few days, a sufficient supply of pizza, and a large-enough white board. A more complete version, across all response types and including decision modelers and other experts, should cost no more than a few million dollars: a small investment to achieve these potential gains. The funding might come from either the DHS National Protection and Programs Directorate's Office of Cybersecurity and Infrastructure Analysis (if the project is best considered an operational issue) or the Science and Technology Directorate's Cyber Security Division (if research).

These response-path maps ought to illuminate how the parallel vectors of response actually unfold, set by step, in order to give the defenders the most advantage, at greatest scale and lowest cost. Once the maps are in hand, government and industry experts can examine each incident class for suggestions on how response could have been more effective: not just how *did* defenders respond, but how *should* they respond next time? Perhaps sharing or declassifying some additional information early enough could have stopped the incident in its tracks. Or, maybe a key response organization lacks sufficient resources, but could dramatically improve with a small grant by DHS or industry, as with the Core Infrastructure Initiative.[5]

Each map can be turned into an appendix for national cyber-incident response plans, leading to a full set of rigorously researched playbooks for all major incidents. Whether in the government or private sector, organizations involved in response can use these playbooks to refine (or create) their own.

Likely, the findings will highlight the massive private-sector role in response, and that many key responders are global organizations, which can help the US government prioritize its efforts with the most effective partners. Beyond these lessons for collaboration, the maps will also provide the actual information requirements—allowing a determination of who needs what information and when, which information needs to be shared, and which information can just be bought (and from what source). These response-path maps may also show that a new kind of organization might help streamline response actions across borders, stakeholders, and sectors.

Piloting New Collaboration Organizations

Much of the current organizational model is built around Information Sharing and Analysis Centers (ISACs), which date back to a 1998 White House policy document. Most ISACs are focused within sectors, and generally within a single country. Seventeen years later, an additional presidential policy created the newer concept of Information Sharing and Analysis Organizations, or ISAOs, to expand sharing beyond specific infrastructure sectors.[6] This ISAO structure could serve as a foundation for organizations focused on collaboration and response. There are already massive efforts underway to respond to incidents, but, "nearly all of the most successful sharing groups share information only incidentally; their core mission is stopping cyberattacks or closing vulnerabilities. So government policy should be equally focused on encouraging groups that solve problems, rather than just sharing information."[7]

A generation of new organizations, perhaps called **Cyber Incident Collaboration Organizations (CICOs)**, could simplify those efforts to make response faster, repeatable, and more streamlined.[8]

---

4 Steve M. Bellovin and Adam Shostack, "Input to the Commission on Enhancing National Cybersecurity," September 16, 2016, https://www.nist.gov/sites/default/files/documents/2016/09/16/s.bellovin-a.shostack_rfi_response.pdf.

5 Core Infrastructure Initiative, "Grants," https://www.coreinfrastructure.org/grants.

6 White House, "Executive Order 13691 of February 13, 2015, Promoting Private Sector Cybersecurity Information Sharing," https://www.federalregister.gov/documents/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing.

7 Healey, *Breaking the Cyber-Sharing Logjam.*

8 Alternate names: Collaboration, Information Sharing, and Analysis Organizations (CISAOs), Operational Coordination Organizations (OCOs), or Cyber Collaboration Organizations (CCOs).

The Conficker Working Group (CWG), which led the response to the Conficker malware between 2008 and 2010, is perhaps the classic example of an ad hoc group that needed to be created from scratch, suffered for resources, and had no legal status. The CWG included volunteer researchers and responders from around the globe, from the public and private sectors. To counter the malware's creators, researchers even needed to use their personal credit cards to register domains the malware would use, for command and control. Perhaps most importantly, the CWG shows that—regardless of how well coordination and response happen—a larger structure can help, and that it is hard to build from scratch in the midst of a crisis.

> "Many small groups, built on trust and the ability to directly affect outcomes, play outsized roles in cyber response."

Many small groups, built on trust and the ability to directly affect outcomes, play outsized roles in cyber response. The technicians involved do so on a volunteer basis, because they care deeply and are in a position to make a difference. Often, their management and corporate counsel may not fully know (or may prefer not to know) the full scope of their involvement. Because these efforts are informal, with no structure, charter, or support team, they may have limited staying power and scale. Other groups, such as the Enduring Security Framework, ICASI, and the more response-focused ISACs may have these trappings, but might benefit from a tighter focus on specific kinds of incidents.[9]

To these ends, a **Counter-Malware CICO** could be built, using the lessons learned from the Conficker Working Group, for a faster, more effective response to such incidents.[10] A **Counter-Botnet CICO** would be similarly global and led by the private sector, with membership including the global organizations that have had the largest role in takedowns—such as, say, Microsoft, FireEye, and the Department of Justice. The **Counter-DDoS CICO** would bring together the global Tier 1 service providers, content-distribution managers, and other organizations that focus on the core Internet infrastructure. This CICO might start with the existing NCC-Communications ISAC, then add in other groups (such as NSP-SEC) that counter DDoS attacks, as well as other governments and non-US providers.

By comparison, the **Counter-APT CICO** might be led and funded by the US government, working with the "Five Eyes" partners (the United Kingdom, Australia, Canada, and New Zealand) and, perhaps, with representation from the Defense Industrial Base and key cybersecurity companies. Much of its work would be classified. Other CICOs might zero in on ransomware, malware outbreaks, or the rapid mitigation of Internet-wide vulnerabilities like Heartbleed.

It may turn out that having one CICO per incident type ends up being too simplistic, or that incidents will be too multidimensional. As one reviewer of this proposal pointed out, how would it respond to "a botnet that is part of a DDoS attack and also is spreading ransomware?" The incident-path maps developed in the first phase ought to help highlight issues like these, and suggest the best organizational model. The idea is to find out where people are already walking, and create the paths to simplify and streamline.

Each CICO would start as an ISAO, which includes operating in line with specific standards, in exchange for liability protection for information shared. Of course, the goal isn't just to share information, but to simplify collective action. The ISAO standards give more than enough flexibility to use them as the foundation for a larger, souped-up collaboration organization. Each would work with appropriate sector organizations. For example, if a particularly vicious DDoS were targeting banks, of course the Counter-DDoS CICO would work with the FS-ISAC. The Department of Homeland Security, especially elements of the National Cybersecurity and Communications Integration Center, would have some role to play in all of these CICOs. In most cases, how-

9 Department of Homeland Security, "Enduring Security Framework," https://www.dhs.gov/keywords/enduring-security-framework; https://www.icasi.org/

10 Conficker Working Group, *Lessons Learned* (Washington, DC: Rendon Group, 2011), http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

ever, that would be merely a supporting role, as the key actions and decisions will be conducted by the private-sector partners.

So, for example, groups already involved in botnet takedowns might come together in a CICO to give themselves a legal entity and liability protection to pour concrete onto a path they've taken together many times. Another model might involve a CICO to specialize in creating small daughter subgroups, on an ad hoc basis, for quick turnkey scale for each new incident. CICOs would need to work with existing ISACs, as part of an overall strategy of taking the path of least resistance.

To succeed, a CICO cannot simply be a new organization with additional overhead. Rather, the goal of a CICO must be to streamline the current response process for an incident type, to provide an umbrella to make such work easier or to upscale it. When the world is hit with the next Conficker, there is no reason for the response team to be so ad hoc that members need to use their personal credit cards. There should be a legal structure, with resources, contact lists, email distribution, and maybe even an executive secretary to keep things moving. There is already significant activity to defeat each of these classes of incidents, so the CICOs need to be developed carefully, purpose built for each kind of response. One size will not fit all.

As one former White House cyber official told the author in response to this proposal, "CIOs and CISOs…already complain about a proliferation of commitments, and regularly point to informal, relationship-driven and very discrete operational collaboration and exchange with peers at other companies as providing the most operational value." CICOs must provide real value, either by reducing the effort involved in the existing response or allowing responses at much greater scale with the same level of effort. If a CICO cannot do this, it should not be created.

Only with a Limited Government Role

DHS might, accordingly, fund and encourage the creation of a pilot CICO for a particularly promising incident class, based on the results of the response-path maps and stakeholder interest. Some initial funding might come from a grant or contract from DHS or another agency. As one model, in 2004, the Financial Services ISAC received a contract of roughly $2 million from the Department of the Treasury to share cybersecurity information to all regulated US financial institutions—no matter how small, and regardless of whether they were formal members of the ISAC.

But, the US government's role probably cannot be much stronger than this, for reasons of perception, collaboration, competence, and ability. New projects, such as the ISACs, are more likely to thrive when they are driven primarily by the private sector. If the private sector sees this as just another government initiative, it may, rightly, be hard to convince that the project will truly focus on its concerns, rather than those of the government. Many private-sector entities will feel burned by past incidents. During Conficker, the response team found the government "had simply taken [its] briefing and presented it at the White House as their own work—and *classified* it, to boot!"[11]

> "If CICOs are primarily created by the US government, they are likely to focus only on US problems and US players."

If CICOs are primarily created by the US government, they are likely to focus only on US problems and US players.[12] To work best, CICOs must collaborate across borders. They might include not just US companies and government, but British, Australian, Japanese, French equivalents—and, yes, even Chinese ones.

Also, the US government probably lacks enough capacity to be the primary implementer of the idea. As another former senior government cybersecurity official said in response to this idea, "DHS still has work to do in support of the new ISAO concept…The historical

11 Mark Bowden, *Worm: The First Digital World War* (New York: Atlantic Monthly Press, 2011).

12 Ibid.

challenge for DHS cyber is that before they can finish a project, they are given a new project (by the Hill, by the White House, by private-sector demand)."

Most importantly, the private sector needs to be the primary mover because, in almost all cases, it is not just the first responder to cyber incidents, but the second, third, and fourth responder as well. It has the greater agility, subject-matter expertise, and the ability to directly "bend" cyberspace through its ownership of the networks. The US government lacks these strengths, but brings other tools to the fight: massive resources, incredible staying power, and additional levers of power. The details will be driven by the incident-class maps, but most CICO structures will start with the private-sector capabilities, and add in these government capabilities where needed.

Toward Collaboration

With so much attention focused on the latest technology, the value of cybersecurity organizations and other process innovations tends to get overlooked. Nearly thirty years ago, after the Morris Worm, the Department of Defense funded the first Computer Emergency Response Team; about twenty-five years ago, Citibank created the first chief information security officer; around twenty years ago, the first ISACs were created, in response to a presidential request, and these were more recently further expanded to ISAOs. The next generation of innovations should simplify agile, scalable response to incidents—across borders, stakeholders, and sectors.

The process should start with deep-dive research to detail the response to different incident classes, to determine who took what decision, based on what information, leading to what action, and with what ultimate result. This disciplined process to create maps of how defenders have previously responded must then drive new organizational concepts, funding, and response plans.

For some, but not all, of these incident classes, a new generation of collaboration organizations could greatly streamline response, allowing faster response, at greater scale and with less effort. Neither of these proposals is particularly complex or expensive, yet they can help make cyberspace far more defensible than it is today.

Jason Healey is a senior fellow at the Atlantic Council's Cyber Statecraft Initiative, a senior research scholar at Columbia University's School of International and Public Affairs, and a former vice chair of the Financial Services Information Sharing and Analysis Center. You can follow his tweets on cyber conflict and cyber risk at @Jason_Healey.

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan 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.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org