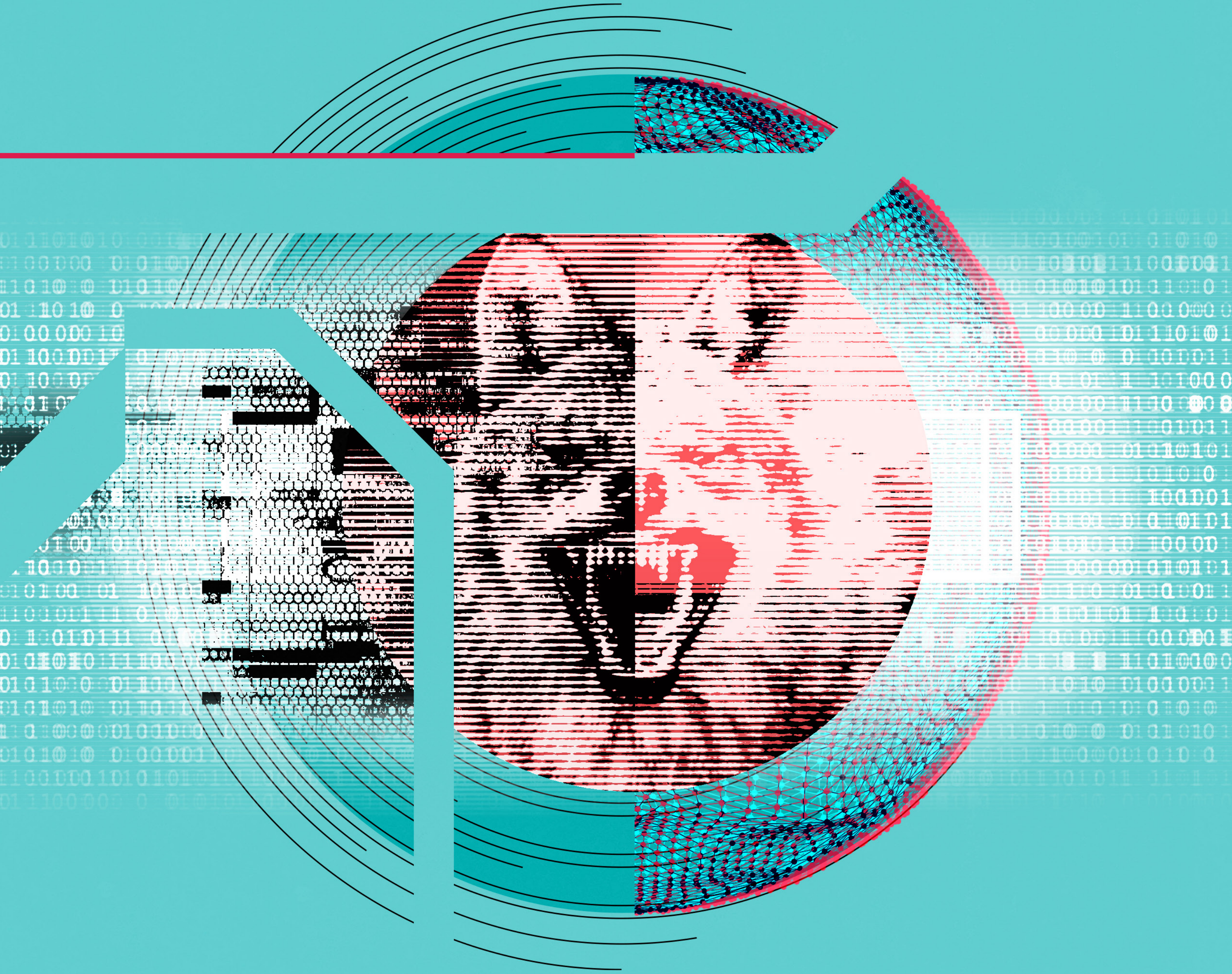
Deloitte.
Insights

A report from the Deloitte
Center for Government Insights



Leading the way with an adversary focus

Government's role in deterring cyber attacks

About the authors

Jesse Goldhammer | jgoldhammer@deloitte.com

Jesse Goldhammer is a managing director in Deloitte & Touche LLP's Cyber and Strategic Risk practice. He builds cybersecurity strategies and programs to safeguard public sector agencies and universities, protecting their data, networks, systems, and people from a wide range of cyber threats. Jesse has worked with the US defense and intelligence communities, US higher education, US philanthropy, and commercial sector clients. He has deep experience in cyber security, strategy, innovation, scenario planning, and workforce training.

Joe Mariani | jmariani@deloitte.com

Joe Mariani is a research manager with Deloitte's Center for Government Insights. His research focuses on innovation and technology adoption for both national security organizations and commercial businesses. His previous work includes experience as a consultant to the defense and intelligence industries, high school science teacher, and Marine Corps intelligence officer.

Matt Stapleton | mstapleton@deloitte.com

Matt Stapleton is a consultant with Deloitte's Government and Public Services practice. His work is within the Defense, Security & Justice sector and is aligned to Borders, Trade, and Immigration clients. He served in the US Navy as an Information Systems Technician (IT) and specialized in cybersecurity and tactical communications.

Akash Keyal | akkeyal@deloitte.com

Akash Keyal is a senior research analyst with the Deloitte Center for Government Insights. He focuses on delivering key insights on topics related to defense, security, and justice.

Adam Routh | adrouth@deloitte.com

Adam Routh is a research manager with Deloitte's Center for Government Insights and a PhD student in the Defense Studies Department at King's College London. His research areas include emerging technologies, defense, and security, with a focus on space policy. Routh previously worked for the Defense Program at the Center for a New American Security (CNAS). Prior to CNAS, he worked in the private sector, where he facilitated training for Department of Defense components. He also served as a team leader with the US Army's 75th Ranger Regiment.

Contents

Responding to exponentially growing cyber threats 2

The forces driving cyber insecurity 4

Cybersecurity needs an adversary focus 6

Coordination at scale creates a tough trade-off 10

The innovations that can break the trade-off 13

Endnotes 16

Responding to exponentially growing cyber threats

IN APRIL 2021, based on a tip from the Federal Bureau of Investigation (FBI) and aided by public sanction data from US Department of Treasury, a social media company took down a massive cross-platform network. The network had been peddling mis- and disinformation, now recognized as a critical national cyber threat. The operation to take down the network is noteworthy not only for its scale—featuring more than 900 websites, social media accounts, groups, and pages across multiple platforms—but also because of how it unfolded: The operation focused on adversaries, not technology, and it took significant coordination to pull off.[1]

Governments face a seemingly inconceivable number of threat vectors, but they can turn them into a manageable problem set by focusing on a small cohort of actors which are responsible for most attacks.

First, the takedown grew out of a focus on bad actors and not on content itself. Governments face a seemingly inconceivable number of threat vectors, but they can turn them into a manageable problem set by focusing on a small cohort of actors which are responsible for most attacks.[2] Tailoring interventions to those bad actors can help push their decision calculus below the threshold of action, deterring attacks before they even occur.

Second, the operation relied on a significant amount of both government-to-government and government-to-industry collaboration. This type of collaboration is not new. Government agencies worked together to counter Soviet propaganda in the 1980s and '90s, and government and industry have shared threat data with each other for years. But recent years have turned the need for that collaboration up to allow more players to coordinate, more information to share, less time to share it. That level of collaboration is often not possible for most government organizations on a day-to-day basis.

Traditional process-defined coordination forces government into a difficult position. It can be agile on a small scale or slow on a large one: Government can coordinate its actions to score a few key wins, but only in a few small areas, such as taking down Trickbot or Emotet botnets.[3] Or government can move quickly in an uncoordinated fashion against more threats, but likely with limited effectiveness. Breaking this trade-off between agility and scale takes innovations based on greater technical and social coordination in government cyber operations.

Innovations for greater collaboration may not grab as many headlines as new technologies or big strategies, but they can help government overcome current barriers to taking a more effective approach to cyberthreats—one that is focused on the adversary. And if successes such as the above operation or defense of the 2020 elections show, an adversary focus is a critical step toward something truly remarkable: a nation more secure from massive cyberattacks.

The forces driving cyber insecurity

THE CYBER LANDSCAPE is being pulled by two seemingly opposed forces: connection and splintering. On one hand, advances in technology are enabling greater connectivity than ever before. On the other hand, national interests such as technology dominance and independence are splintering that connectivity into balkanized zones.

Technology is driving greater connection

The proliferation of smartphones has brought the internet to all of our pockets, but it is the explosion of small Internet of Things devices where the world's growing connectivity can be most clearly seen. There are already more than 13 billion internet-connected devices on the planet, and this number is growing 10 times faster than the human population.[4] These devices are bringing connectivity to previously disconnected items, such as water pumps and factory machine tools, allowing for previously unheard of agility and efficiency but also increasing the cyberattack surface of many organizations.

Greater connectivity is not only linking devices, it is also making organizations more intertwined than ever before. Take cloud as an example. Today, more than 94% of enterprises are in the cloud.[5] And it is not just small-scale explorations; 83% of all enterprise workloads are estimated to be in the cloud today.[6] The result is that many organizations are becoming increasingly reliant on not just their cloud service provider, but also the service and technology vendors on which their cloud provider relies.[7] Technology is creating interdependencies that can introduce unseen vulnerabilities ripe for adversaries to exploit.

Technology is creating interdependencies that can introduce unseen vulnerabilities ripe for adversaries to exploit.

Nations are driving the greater splintering

Pulling in the opposite direction of technology-driven connectivity is greater splintering. The balkanization of the internet that has been underway for over a decade has resulted in different technical ecosystems cropping up. Russia and China, isolated by their Sovereign Internet Law and Great Firewall, respectively, have developed very different technical ecosystems.[8] So when the trend toward centralization takes place in these countries, the data is being centralized by a very different array of companies using different technologies than most of the world. For example, Amazon and Microsoft are the top two infrastructure-as-a-service providers, accounting for about 63% of the entire global market. Yet, they are nowhere to be found in Russia, where Softline, Rostelecom, and MTS lead the market; and in China, Amazon comes in a distant fourth, and Microsoft ninth, behind Alibaba, Tencent, and China Telecom.[9]

Splintering is encouraging some of the most capable cyberthreats

The trend toward balkanization of tech ecosystems appears to be changing the decision calculus of several US adversaries. With very different technical ecosystems, US adversaries can craft cyberattacks with greater—although not perfect—assurance that those attacks will not rebound and disrupt their own domestic networks.[10] In other words, it is easier for an adversary to choose to attack a piece of software/hardware if it is not used on networks in their own country. So, balkanization of technology increases the opportunities for cyberattacks while somewhat decreasing the risk of those attacks. Greater potential reward and less risk are likely drivers behind what the Office of the Director of National Intelligence called "states' increasing use of cyber operations as a tool of national power."[11] Recent attacks on everything from water treatment plants to gasoline pipelines show just how powerful a tool those attacks can be.[12] With such an attractive tool of national power, analysts in government and industry expect more attacks and more aggressive attacks that may even impact civilians.[13]

With very different technical ecosystems, US adversaries can craft cyberattacks with greater—although not perfect—assurance that those attacks will not rebound and disrupt their own domestic networks.

Cybersecurity needs an adversary focus

THE SHIFTING TECHNOLOGICAL landscape has fundamentally altered when and how adversaries decide to attack. Therefore, governments' approaches to cyber defense needs to address this decision calculus if it hopes to create effective defenses.

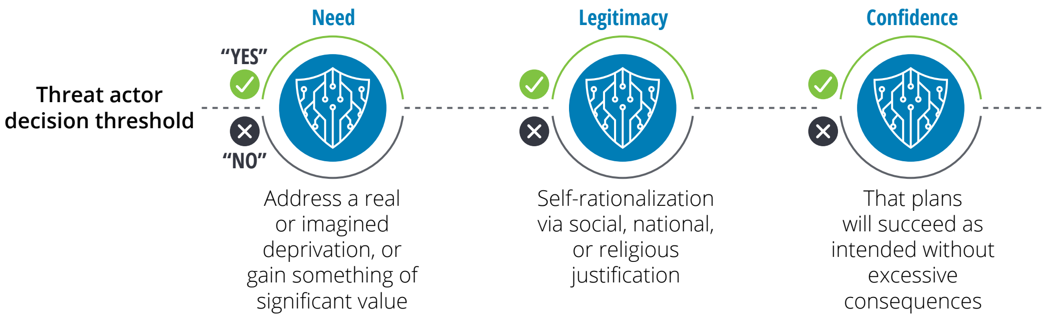
To defend against the most capable cyberthreats, defenders should focus on the actors with the greatest capability and intent to attack. Typically, those will be large, adversarial nation states.[14] For the rest of this paper, we will largely focus on the threat posed by adversarial nation states, but that does not mean that other bad actors such as cybercriminals, hacktivists, or others are ignored. Rather, once government adopts an adversary focused approach to cyber defense, the same approach can be used on a variety of actors. For example, the self-shutdown of ransomware-as-a-service syndicate DarkSide amidst growing public pressure and law enforcement seizures shows just how the combination of enforcement actions and messaging can push even criminal decision-making in a positive direction.[15]

But the bottom line is to effectively counter today's threats, governments need to be able shift the decision calculus of attackers: keep them below the threshold of deciding to attack. To do this, governments need to understand the criteria adversaries use to justify an offensive cyber operation.

If an adversary is debating whether to conduct a cyberattack, it needs three different factors to rise above its decision threshold (figure 1).[16] There must

FIGURE 1

Adversary decisions to attack are driven by their perceptions of need, legitimacy, and confidence


Need
Legitimacy
Confidence
"YES"
Threat actor decision threshold
"NO"
Address a real or imagined deprivation, or gain something of significant value
Self-rationalization via social, national, or religious justification
That plans will succeed as intended without excessive consequences

Source: Based on Deloitte analysis of Cyber Solarium Commission Report and Chris Demchak, *Wars of Disruption and Resilience*, (Athens, GA: University of Georgia Press, 2011).

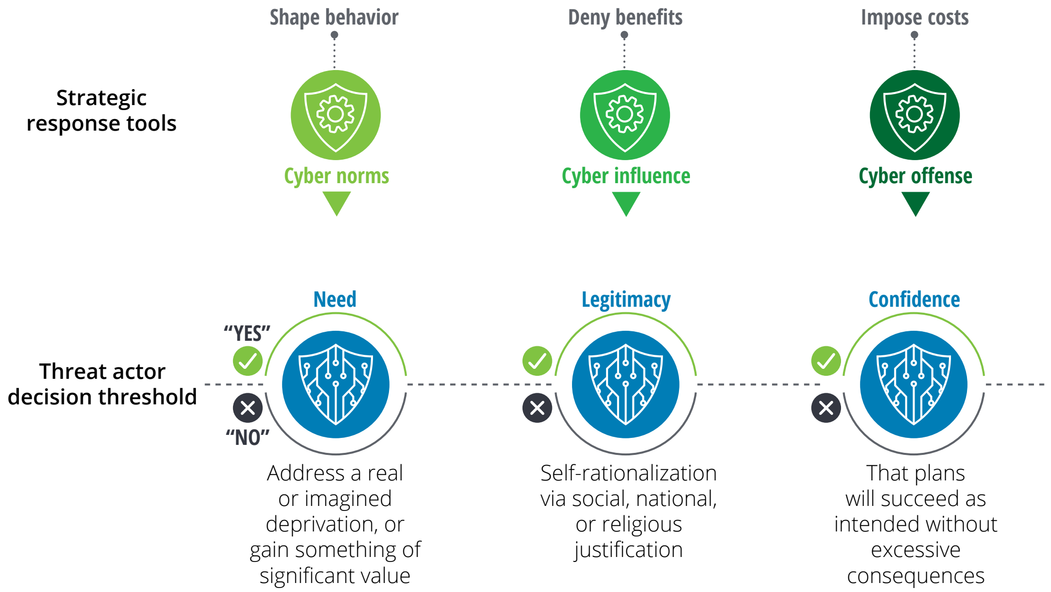
be some *need* to attack. This can be pragmatic gain such as money or territory, punishment for a past wrong, or nearly anything else of value. Next, the actor must be satisfied that its actions are legitimate. This does not mean legal, but internally justifiable. After all, spies, by definition, break the laws of other countries, but they are typically quite careful to make sure their actions fall under domestic laws and their own individual morals. Finally, adversaries need to have confidence that the attack will succeed and not result in even worse consequences from unintentional bounce-back or retaliation.

> **In some sense, the adversary focused approach to cyber shifts much of the burden of cyber defense "left of click" to prevent the most devastating attacks.**

This framework of adversary decision calculus is also incredibly useful to cyber defenders. To deter or prevent attacks, government needs to push an adversary's thinking on any of those factors below the decision threshold (figure 2).[17] Rather than playing "whack-a-mole" with the huge number of threats and vulnerabilities, governments can deploy several actions in advance to deter the most threatening adversaries from attacking in the first place. In some sense, the adversary focused approach to cyber shifts much of the burden of cyber defense "left of click" to prevent the most devastating attacks.

FIGURE 2

Matching government actions to each aspect of adversary decision-making can help deter cyber attacks


Shape behavior
Deny benefits
Impose costs
Strategic response tools
Cyber norms
Cyber influence
Cyber offense
Need
Legitimacy
Confidence
"YES"
"NO"
Threat actor decision threshold
Address a real or imagined deprivation, or gain something of significant value
Self-rationalization via social, national, or religious justification
That plans will succeed as intended without excessive consequences

Source: Based on Deloitte analysis of Cyber Solarium Commission Report and Chris Demchak, *Wars of Disruption and Resilience*, (Athens, GA: University of Georgia Press, 2011).

An adversary focused approach seeks to shape behavior, deny benefit, and impose costs on an adversary to deter it from launching cyberattacks. If adversaries first require a *need* for an attack, government's first action should be to use technology standards and other tools to **shape behavior**. The core values baked into standards tend to become the norms of behavior in a technological environment. The underlying beliefs of "free exchange of information" that underpinned the early days of the internet were codified in technology standards such as TCP/IP protocols, which, in turn, helped shape norms of real people's information-sharing behavior as the World Wide Web took shape. Governments can use similar standards and norm-setting bodies to encourage desirable and minimize negative behavior in cyberspace. Of course, standards just set the "default" behavior, so to speak, and adversaries are always free to act differently. In that case, cyber influence operations can promote messages that directly undercut an adversary's motives. By removing the all-important sense of legitimacy, cyber influence can **deny attackers the benefit of an attack**. Finally, if the adversary still finds a need and a legitimate motive, cyber offense can preemptively degrade an adversary's capability for attack or threaten to **impose costs** such that it no longer has confidence that it can get away with any attack unscathed.

In some sense, the adversary focused approach to cyber shifts much of the burden of cyber defense "left of click" to prevent the most devastating attacks.

The challenge is that, in most governments, these actions are often split across many different agencies and authorities (figure 3). For example, in the United States, standard- and norm-setting is the domain of agencies such as the National

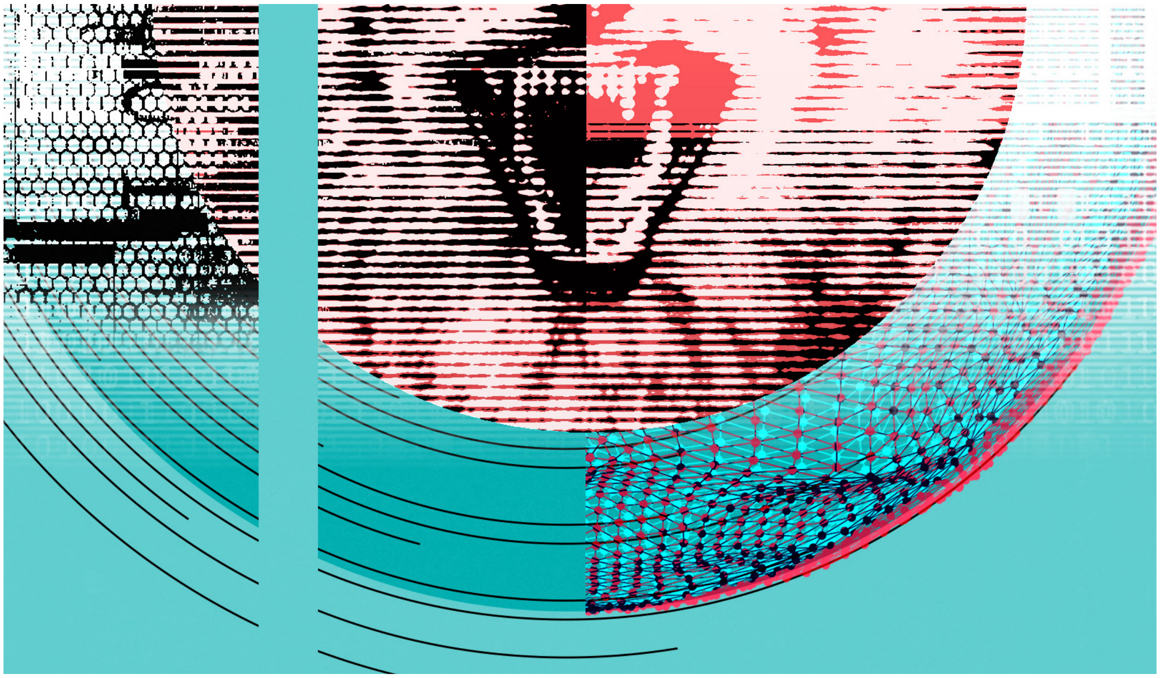
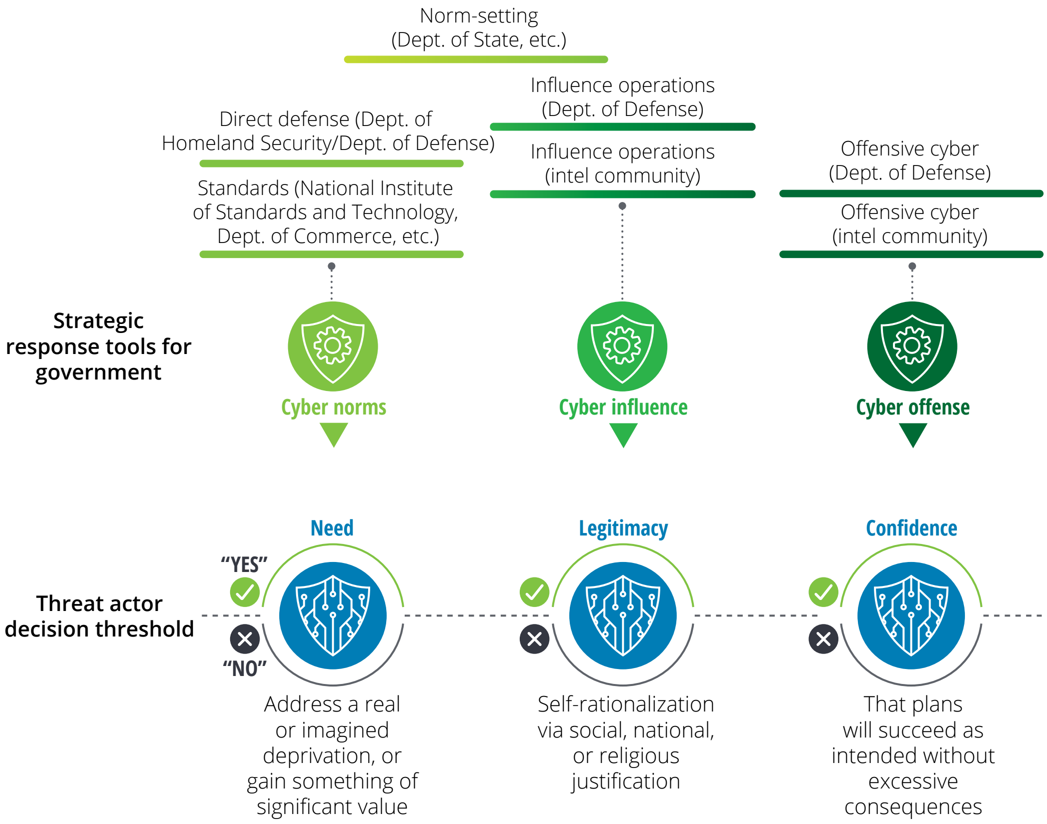


FIGURE 3

Effective deterrence depends on coordinating many different agencies, roles, and authorities, all at the speed and scale of cyber


Norm-setting (Dept. of State, etc.)
Direct defense (Dept. of Homeland Security/Dept. of Defense)
Standards (National Institute of Standards and Technology, Dept. of Commerce, etc.)
Influence operations (Dept. of Defense)
Influence operations (intel community)
Offensive cyber (Dept. of Defense)
Offensive cyber (intel community)
Strategic response tools for government
Cyber norms
Cyber influence
Cyber offense
Threat actor decision threshold
"YES"
"NO"
Need
Legitimacy
Confidence
Address a real or imagined deprivation, or gain something of significant value
Self-rationalization via social, national, or religious justification
That plans will succeed as intended without excessive consequences

Source: Based on Deloitte analysis of Cyber Solarium Commission Report and Chris Demchak, *Wars of Disruption and Resilience*, (Athens, GA: University of Georgia Press, 2011).

Institute of Standards and Technology, Department of State, Department of Commerce, and others. Cyber influence and cyber offense can be within the domain of either the defense or intelligence communities, each operating with very different restrictions and authorities.

In an effective adversary focused strategy, tech standards, norms, influence, and offense all need to be calibrated to push a specific adversary's decision calculus below the threshold of action. All this needs to happen at speed and while respecting the laws and liberties of each area where agencies operate. That level of coordination is hard for most government organizations. Achieving it at the speed and scale of cyberspace in the current system is near-impossible.

Coordination at scale creates a tough trade-off

INTRAGOVERNMENTAL COORDINATION MAY seem like an obvious answer when adopting an adversary focused approach to cyber, but it has one major challenge: it is difficult to do at the necessary scale. Intragovernmental coordination can be complex even at a small scale, so when issues grow in size and speed, the complexity of the coordination required increases exponentially.

Take the Active Measures Working Group (AMWG) as an example. Formed in the 1980s to counter Soviet propaganda, the AMWG brought together subject matter experts from the US State Department, the US Information Agency, the CIA, the FBI, and even congressional staffs. The group worked as an information broker across the federal government to identify, track, and develop strategies to successfully counter Soviet disinformation campaigns in the United States and abroad.[18] This level of coordination across conference tables was sufficient to successfully counter the disinformation being spread through newspapers and media placements. While those media could achieve significant global reach, as seen in the Soviet misinformation campaign proffering that AIDS was created in US government labs, the spread of specific messages was slow. It took over a year from the first appearance of a falsified scientific report for the story to spread to its ultimate audience in 80 countries.[19] Contrast that with the speed with which online conspiracy theories about COVID-19 spread, some of which reached audiences of more than 6 million in less than 24 hours after posting.[20] The conference table coordination of AMWG simply would not be able to keep up with that pace. Add on top of that the growing number of participants would need to coordinate with tech companies, telecommunications regulators, and health and science experts, in addition to cyber and national security agencies, and it is nearly impossible in the current model to achieve the coordination necessary.

In essence, what government faces is a trade-off between agility and scale.

Nor are these issues with coordination limited only to the fight against mis- and disinformation. The same complexities hamper defending against cyber espionage and other purely cyber operations as well. Public reporting highlights how early offensive cyber operations such as Operation Glowing Symphony were hampered by slow decision-making and inefficient mechanisms of coordination.[21] These challenges are not just historical accidents. Rather, they show that the scale of today's cyber problems run into organizational barriers that keep government from fully adopting an adversary focused approach to cyber. (See sidebar "The organizational barriers to an adversary focused approach" for a fictional vignette about cyber operations in great power competition.)

THE ORGANIZATIONAL BARRIERS TO AN ADVERSARY FOCUSED APPROACH: A FICTIONAL VIGNETTE OF SPECIAL OPERATIONS INFLUENCE OPERATIONS

Special Operations Task Force 427 has become the poster child for influence (or information) operations (IO). The team has built a string of tactical successes by focusing on the thinking of its adversaries and closely coordinating to make sure its actions can influence that thinking.

Master Sergeant Alonto is an often-cranky career Green Beret whose years of experience working in Southeast Asia have made him a human data center with nuanced insights into certain Asian communities. MSG Alonto's knowledge is invaluable to Captain Jessica Bluff, who must generate persuasive content as the leader of the task force's tactical psychological operations team. A savvy cyber team is the final part of the dream team, delivering CPT Bluff's content to specific individuals and groups through offensive cyber operations. The team merges individual capabilities to successfully shape local public perception in support of US and allied political, social, and economic beliefs—most aptly shown in its most recent mission to rally support for Freedom of Navigation operations in the South China Sea within a small but important fishing community.

Hoping to replicate the team's success across a larger swath of Southeast Asia, headquarters back in Hawaii orders the team to begin working on regional issues. The team quickly realizes that in IO, success doesn't scale as quickly as problems do. The team works hard, but, just as it is beginning to make headway in one small island chain, a crisis crops up in another set of islands. Faced with a relatively unknown target population and cyber situation, and unable to reshuffle resources quickly enough, the team can only fire off a few largely ineffective messages before the crisis has passed.

The after-action report identifies four main problems that limited how successful even a star tactical team could be when faced with challenges of larger scale:

- **Complexity**—The environment facing the team at a tactical level was complicated, but not complex. There were a number of players to keep in mind, but with simple organization and visualization tools, the team could devise strategies to work for each. At an operational or strategic level, not only are there more players but also more interdependencies between them. The result is exponentially more complexity that cannot be visualized on a piece of paper or slide deck.
- **Fragility**—Currently, the precise local knowledge needed to craft and deliver impactful messages is only available from individual Special Forces contacts and cyber reconnaissance tools. These mechanisms are powerful but fragile, and therefore prone to failure when personnel rotate or missions suddenly change.
- **Fixedness**—Resource allocation processes are more fixed than the operating environment. Taskings and assignments are made up to months in advance, so when a rapidly shifting situation changes the target or moves up a timetable, getting the right resources can be near-impossible.
- **Vulnerability**—Finally, the scale and speed of great power competition expose a vulnerability in command authorities. The potential blowback of tactical level IO is an important consideration, but it takes on entirely new proportions when great power messaging can touch on sensitive diplomatic issues or even impact global trade. This significantly shifts decision-maker calculus, making leaders more risk-averse at the strategic scale than they are at the tactical.

These four factors represent key organizational barriers keeping government from adopting adversary focused approaches at the scale needed.

In essence, what government faces is a trade-off between agility and scale. Agencies can be quick and responsive at a small scale, like the AMWG was, but growth often requires bureaucratic processes that stifle speed. The problem is that today's cyber threats demand both agility and scale. Those threats operate on timescales that demand agility, and at the same time can touch so many aspects of life that they require significant coordination within and outside of government. An effective response to these threats may require input from law enforcement, intelligence agencies, telecommunications regulators, and private industry. Achieving that level of coordination on the timescales required to change the adversarial decision calculus puts government in a double bind: It can respond effectively, but late; or respond on time, but in a manner that is uncoordinated and likely ineffective.

The agility versus scale trade-off means that if government is to adopt an adversary focused approach to cyber, it must first start with some internal innovations that can break that trade-off. Government agencies and commercial companies alike have found ways to break the trade-off and be agile at scale.[22] Those innovations can allow government to coordinate at the speed and scale required by the adversary focused approach.

The innovations that can break the trade-off

INNOVATIONS ARE NOT restricted to merely new technologies. One textbook definition of an innovation is anything that breaks a trade-off.[23] The innovations government needs to achieve coordination at the speed and scale required for adversary focused cyber can be anything from new technologies to new strategies to new business practices.

Government has been slowly discovering some of those innovations as it tentatively explores scaling cyber missions. New doctrines such as "defend forward" and "persistent engagement" can be seen in the long tradition of doctrinal innovations in national security.[24] Similarly, new organizations such as the Cybersecurity and Infrastructure Security Agency and US Department of Defense cyber mission teams helped to resolve difficult trade-offs as organizations assumed new cyber missions.

Government has been slowly discovering some of those innovations as it tentatively explores scaling cyber missions.

Yet, the innovations deployed so far don't sufficiently address adversaries' decision threshold. The adversary focused approach to cyber demands coordination across all government agencies that exercise national cyber power. But since the challenges of scale—complexity, fragility, fixedness, and vulnerability—stand in the way of achieving that coordination at the speed and scale required, government needs innovations that can tackle each one.

Reducing complexity: AI-human teaming

In older eras, commanders could use maps or spyglasses to easily see where their forces were and where the enemy was attacking. Today's cyber leaders have the same need, but with billions of internet end points, no human mind can contain all of the information needed. What is needed is technological innovation bringing together artificial intelligence (AI) and data visualization to make vast volumes of cyber data digestible to human leaders. Tools such as Project IKE, a tool developed by the Defense Advanced Research Projects Agency (DARPA) that is newly deployed to US Cyber Command, can collate and curate the right data, allowing 3D visualization software such as Immersive Wisdom to literally 'show' human operators the nonphysical environment of cyberspace. With those tools, human operators can spend less time sifting through network data and more time making mission decisions much as intelligence analysts are beginning to do today with AI.[25]

Reducing fragility: A real-time shared picture for faster decision-making

Fragility is really a problem of agility. Highly efficient processes often cannot adapt quickly enough to changing circumstances. If government wishes to reduce fragility in cyber decision-making, it needs to speed the pace of its own decision-making, across all the agencies involved.

Countering fragility is really a two-step process: First, all agencies need a real-time shared picture of the world; and second, leaders need decision supports to help them formulate courses of action in such a complex world. Creating a real-time, shared picture of the cyber environment is difficult not only because of the complexity of the environment, as discussed above, but also because much of the data will be highly classified and hard to share. But solutions to these problems already exist. For example, cross-domain intelligence-sharing can help create an environment where agencies can seamlessly make data discoverable to those who need it and have a right to access it.[26] Then, with a shared understanding of the operating environment, leaders need decision supports to help them understand how their actions will impact the adversary and even the plans of other agencies. For example, how will an offensive cyber operation impact the adversary or degrade ongoing influence operations? AI can again help with these questions, as demonstrated by DARPA's Deep Green program more than a decade ago, but ultimate success depends on all cyber leaders working from a common picture toward a shared goal.[27]

Reducing fixedness: National leadership

If faster decision-making depends on leaders sharing a common picture and common goals, technology can help with the common picture, but common goals can come only from unified leadership. Some central cyber leadership structure is necessary, whether on the national security council staff or as a stand-alone executive position. This central leadership can produce a coherent vision for the exercise of national cyber power so that each agency can act quickly on its own initiative but still stay assured that their collective actions are helping achieve larger ends.

More than just a strategy document, cohering around common goals is about creating common organizational culture. Government is no stranger to creating common cultures from many diverse organizations. Organizations such as the Office of the Director of National Intelligence and legislation such as the Goldwater-Nichols Act have helped create communities out of individual agencies. National cyber leadership can serve a similar role in building social coordination on cyber via rotational assignments, joint duties, common training curricula, and more.[28]

Reducing vulnerability: Make vulnerabilities visible

A nation's cyber vulnerabilities often arise from hidden interdependencies. Government may not be aware of who is making its technology, and companies may not be aware of whom they are depending on for their hardware and services. Making all of these interdependencies visible can help leaders in both government and industry take appropriate actions to mitigate the risk, essentially shaping the norms of the cyber environment.

Supply chain illumination tools can share details on government suppliers, and their suppliers in turn, down several tiers, to help see what is really going into their technology. Similarly, mandatory disclosure laws can help ensure that once vulnerabilities are identified in commercial products, they do not spread unseen and compromise even more organizations. These changes may be uncomfortable at first for both government and industry, but they represent the first steps toward a mindset of collective defense. The mindset that we are so interconnected we are all in this together is the cornerstone for reducing vulnerability in a complex cyber environment.

Technology is always advancing, and there will always be new vulnerabilities. What matters most is the capability and intent of adversaries to exploit those vulnerabilities. Therefore, long-term cybersecurity rests on government's ability to coordinate all the functions of national power against the decision calculus of each adversary. But to do that coordination at the speed and scale required takes new innovations in government technology and organization. With those innovations, governments can do what today seems impossible: live in a world free of massive cyberattacks.

Endnotes

1. Facebook, April 2021 Coordinated inauthentic behavior report, accessed June 12, 2021.
2. Vibhor Sehgal, Ankit Peshin, Sadia Afroz, and Hany Farid, *Mutual hyperlinking among misinformation peddlers*, April 26, 2021.
3. For more see Department of Justice, “Emotet Botnet disrupted in international cyber operation,” January 28, 2021; and Ellen Nakashima, “Cyber command has sought to disrupt the world’s largest botnet, hoping to reduce its potential impact on the election,” *The Washington Post*, October 9, 2020.
4. Lionel Sujay Vailshery, “Internet of Things (Iot) and non-IoT active device connections worldwide from 2010 to 2025,” Statistica, March 8, 2021.
5. Nick Galov, “Cloud adoption statistics for 2021,” January 19, 2021.
6. Louis Columbus, “83% of enterprise workloads will be in the cloud by 2020,” *Forbes*, January 7, 2018.
7. Anna Dubois, Kajsa Hulthen, and Ann-Charlott Pedersen, *Interdependence within and among ‘supply chains,’* IMP Group, accessed June 12, 2021.
8. Anton Troianovski, “China censors the internet. So why doesn’t Russia?,” *New York Times*, February 23, 2021.
9. For estimates of Russian IaaS market see: https://www.cnews.ru/reviews/oblachnye_servisy_2020/articles/rejting_cnews_iaas_spros_na_infrastrukturu For the Chinese market see: https://www.sans.org/blog/doing-cloud-in-china/
10. For an example of the imperfect nature of this assurance, see the impact of the NotPetya malware, widely attributed to Russia’s GRU, on Russia itself. However, it is useful to remember that the NotPetya attack occurred in 2017, before Russia’s Sovereign Internet Law was passed in 2019.
11. Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Committee*, April 9, 2021.
12. For the potentially deadly outcome of water treatment hack see: https://cen.acs.org/environment/water/water-treatment-plant-hack-affected/99/web/2021/02 and for pipeline hack see: https://www.wsj.com/articles/web-site-of-darkside-hacking-group-linked-to-colonial-pipeline-attack-is-down-11621001688
13. For ODNI’s impact on intelligence culture see: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf; for assessments from commercial analysts see: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf
14. US Department of Homeland Security, "Testimony to the House Homeland Security Committee,” Feb. 10, 2021.
15. KrebsonSecurity, “Darkside ransomware gang quits after server’s bitcoin stash seized,” May 14, 2021.
16. Chris Demchak, *Wars of Disruption and Resilience: Cybered conflict, power, and national security*. The University of Georgia Press. Athens, GA. 2011.
17. US Cyberspace Solarium Commission, “Report,” March 2020.
18. Fletcher Schoen and Christopher J. Lamb, “Deception, disinformation, and strategic communications,” Institute for National Strategic Studies, Strategic Perspectives 11, 2012.
19. Douglas Selvage and Christopher Nehring, *Operation Denver: KGB and Stasi disinformation regarding AIDS*, The Wilson Center, July 22, 2019.

20. David Klepper, Farnoush Amiri, and Beatrice Dupuy, “The superspreaders behind top COVID-19 conspiracy theories,” *AP News*, February 14, 2021.

21. Joseph Marks, "The Cybersecurity 202: Here’s the inside story of Cyber Command's campaign to hack ISIS," *The Washington Post*, January 21, 2020; Dustin Volz, "How a military cyber operation to disrupt Islamic state spurred a debate," *The Wall Street Journal*, January 21, 2020.

22. Deloitte, *How innovation in government can help break trade-offs and improve services*, Deloitte Insights, November 15, 2021.

23. Deloitte, *Innovation: A chimera no more*, Deloitte Review Issue 13, July 25, 2013.

24. Deloitte, *The blueprint for a better military*, Deloitte Insights, 2021.

25. Mark Pomerleau, “A cyber tool that started at DARPA moves to Cyber Command,” C4isrnet, April 20, 2021 and PRNewsWire, “Immersive wisdom connects four geographically distributed sites in real time on siprnet within its real time 3D geospatial collaboration platform in significant achievement for air force advanced battle management system (ABMS) OnRamp #2,” news release, September 8, 2020.

26. The progress in cross-domain and industry collaboration made by many members of the Intelligence Community during the COVID-19 pandemic has been a great example of what is possible albeit in small scale. For example, see https://defensesystems.com/articles/2020/11/18/ai-geoint-covid.aspx

27. Defense Industry Daily staff, “DARPA’s commander’s aid: From OODA to deep green,” Defense Industry Daily, June 3, 2008.

28. For more on the impact of Goldwater-Nichols on defense culture see: https://www.jstor.org/stable/2657652?seq=1; for ODNI’s impact on intelligence culture see: https://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf

Acknowledgments

The authors would like the thank **RADM (Ret) Mark Montgomery**, **John Costello**, and **Robert Morgus** of the Cyber Solarium Commission for generously sharing their expertise and insight.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Tim Li
Government and public services cyber strategic growth leader | Principal | Deloitte Consulting LLP
+1 240 205 2474 | timli@deloitte.com

Tim Li is a principal at Deloitte & Touche LLP and the Government & Public Services industry Strategic Growth Offering leader for Cyber.

Mark Nace
Government and public services cyber & strategic risk leader | Principal | Deloitte Consulting LLP
+1 703 499 2278 | mnace@deloitte.com

Mark Nace is a principal at Deloitte & Touche LLP and Government & Public Services leader for the Cyber & Strategic Risk practice of Deloitte Risk & Financial Advisory.

Jesse Goldhammer
Cyber and strategic risk | Managing director | Deloitte Consulting LLP
+1 510 219 5760 | jgoldhammer@deloitte.com

Jesse Goldhammer is a managing director in Deloitte & Touche LLP's Cyber and Strategic Risk practice.

The Deloitte Center for Government Insights

Joe Mariani
Research manager | Deloitte Services LLP
+1 240 731 1985 | jmariani@deloitte.com

Joe Mariani co-leads Deloitte's research in justice, defense, and intelligence for Deloitte's Center for Government Insights.

About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what’s behind the adoption of new technologies and management practices. We produce cutting edge research that guides public officials without burying them in jargon and minutiae, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

Government & Public Services Cybersecurity

Digital transformation, enabling technologies, and connected communities are expanding and adding complexity to attack surfaces. Organizations should identify where cyber risks need to be addressed across mission ecosystems and elevate cyber programs with new techniques. These approaches can better support and protect your mission. Deloitte collaborates with organizations to provide deeper insight into addressing cyber risks while promoting innovation and mission impact. To learn more, visit Deloitte.com.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Aditi Rao, Aparna Prusty, and Emma Downey
Creative: Govindh Raj and Sonya Vasilieff
Audience development: Alexandra Kawecki
Cover artwork: Stephanie Dalton

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.