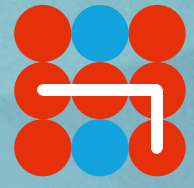
COI STRATEGY & DEFENCE

Hybrid CoE Paper 10

DECEMBER 2021

Cyber conflict in a hybrid threat environment: Death by a thousand cuts

WILLIAM E. LEIGHER



Hybrid CoE

Hybrid CoE Paper 10

Cyber conflict in a hybrid threat environment: Death by a thousand cuts

WILLIAM E. LEIGHER

Hybrid CoE Papers are finalized pieces of analysis on a topic related to hybrid threats, based on one or several research questions. They may be either conceptual analyses or based on a concrete case study with empirical data.

COI Strategy & Defence focuses on hybrid warfare, related strategies and resulting implications for security policy, military and defence. It aims at discovering the essence and nature of hybrid warfare as well as the logic and pattern of hybrid strategies in order to develop an analytical framework for the assessment of current and future hybrid warfare situations.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN (web) 978-952-7472-02-6
ISBN (print) 978-952-7472-03-3
ISSN 2670-2053

December 2021

Hybrid CoE is an international hub for practitioners and experts, building Participating States' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats, located in Helsinki, Finland.

Contents

Introduction

Much of the commentary and the fictional accounts about cyber warfare involve a surprise attack that has been coordinated to take advantage of a nation's specific weakness in cyberspace. Likewise, discussions about a nation-state's employment of cyber forces focus on their potentially offensive roles. There are a range of scenarios describing the international political and social environments between now and 2040 that describe contentious national security environments,[1] and a statistical review of conflicts indicates that the world could be "due" for a war between major powers.[2]

While taking this into consideration, national security theorists and planners are notoriously bad at predicting future events, and the likelihood of a war between major powers or military alliances in the next twenty years is probably low. Should this be the case, the challenge for cyber-security planners, as it relates to countering cyber-based hybrid threats, will be to optimize cyber defences for this environment. The likely scenario for cyber defence is countering attacks similar to those that have occurred between 2010 and 2020 – but with a greater number of events and increasingly complex exploits. This positions cyberattacks and cybercrimes as the most prominent part of a hybrid threat campaign for the next two decades. The damage inflicted by the many small cuts from current cyberattacks is like the human equivalent: a slow and lingering punishment. This could elevate cyber security as the most significant national security challenge to be faced over the next couple of decades.

This paper puts these nation-state-sponsored cyber warfare actions into perspective as compared to cyber actions used for espionage or cybercrime. A brief review of the attacks that have been attributed to a specific nation demonstrates how the complexity, severity, and cost have increased over the last two decades. Lastly, the examples show how both national security policy and cyber-security practices should change to counter looming cyber defence challenges.

1 Office of the Director of National Intelligence. The National Intelligence Council, 'Global Trends 2020: A More Contested World' (Office of the Director of National Intelligence, March 2021), https://www.dni.gov/files/images/globalTrends/GT2040/GT2040-Foreword.pdf, 6. This report by the US Office of the Director of National Intelligence is one of many scenario-based documents which forecast a volatile global national security environment for the next two decades. These reports do not predict a major conflict, but only highlight those contentious environments that exist. [Unless otherwise indicated, all links were last accessed on 29 September 2021.]

2 Aaron Clauset, 'Trends and Fluctuations in the Severity of Interstate Wars', *Science Advances*, Volume 4, Issue 2 (2018): pp. 1–9, https://doi.org/10.1126/sciadv.aao3580. The paper does not predict a war, but only indicates that statistically the world is due for a major war.

Three categories of offensive cyber actions

Western democracies form militaries for defensive purposes, and alliances are generally defensive in nature. However, there is always a balance between defensive needs and the firepower necessary to respond to an attack. Cyber warfare is no different. Since nations began creating cyber forces as a part of military services in the late 2000s, much of the emphasis has been on offensive cyber operations. Perhaps this is because of the military nature of the forces – defensive operations rarely come to mind first when one thinks of the application of military force. Additionally, nearly every cyber event in the news is labelled a cyberattack.

It is worth restating that offensive cyber actions fall into three broad categories. First is the use of cyber as a means of spycraft to conduct espionage. While one could simply point out that many nations do this, it is not generally conducted with the explicit aim of destroying or disabling a remote target. The second is cybercrime, activities that use cyber means to extort, fraudulently obtain, or flagrantly steal assets. But again, like espionage, cybercrime is not committed with the goal of destroying property, although ransomware often threatens the destruction of data, which may be extremely costly. The third is cyber warfare, where the goal is to destroy or disable a target, using cyber operations to achieve political ends. The cyber exploits used in support of intelligence-gathering and criminal cyber activities are common. Cyber warfare, however, is not. Since cyber exploits were first used as an element of national power, only a handful of events have occurred that would qualify as cyber warfare. The increasing complexity of cyberattacks makes it difficult to quickly assess the long-term impact. Cyber events like SolarWinds may have hostile intent, but it could take months to comprehend the extent of the damage.

The interrelationships between these three areas of offensive cyber is what produces the grey and shadowy aspects of cyber operations. Offensive cyber operations depend on exploiting software or weaknesses in cybersecurity. Of all the difficulties in understanding the ongoing cybersecurity environment, determining the root cause of the penetration and long-term intent of the attacker is perhaps the biggest challenge for nations and cybersecurity professionals.

This is an interesting scenario for hybrid warfare. Consider a situation where a steady stream of cyber “attacks” are occurring. They are taking place below the threshold of what might cause a retaliatory strike, whether the response is by cyber means or employs a traditional kinetic attack. The escalation of cybercrime and cyberattacks, both in complexity and impact, during the past fifteen years has been very costly, and is an area where the policy and legal framework is immature and unprepared.

Record of global cyberattacks

A brief review of instances where cyber events appear to have been state sponsored shows the danger and impact of limited attacks, even in the absence or likelihood of a major conflict between superpowers. Cyberattacks, when viewed individually, are seen as limited in scope and not serious national security threats. However, when looked upon as part of a hybrid threat campaign designed to influence, undermine policies, and carry out state and commercial espionage, the cumulative impact and cost are significant. The history of state-based attacks, that is cyberattacks that have been attributed to a specific country, demonstrates the growing damage and fiscal costs incurred, as seen in the Estonia, Ukraine, Iran, Saudi Aramco, NotPetya and SolarWinds (both of which were multinational) cyber events. Cyberattacks can have an impact by spreading quickly to unintended remote targets. This was seen in a July 2021 ransomware attack, where the software of Kaseya, a global IT infrastructure provider, was used to deliver the ransomware during an update for its customers. The history of the last 15 years shows that a nation employs cyber options when it wants to obfuscate the source of an attack or when it is unable or unwilling to use normal means of power.

Estonia suffered a denial-of-service (DoS) attack over the course of a month in April and May 2007. This is widely seen to have been a punitive attack by Russia when Estonia relocated a statue that memorialized World War II soldiers. The Russian government was assisted by, or even depended upon, a private entity, the Russian Business Network, to execute the DoS attack. In addition to rioting and violence from April 27 to May 18, distributed denial-of-service (DDoS) cyberattacks targeting the country's infrastructure shut down the websites of all government ministries, two major banks, and several political parties. At one point, hackers even disabled the parliamentary email server.[3] The estimated cost to the financial services sector was approximately one million dollars,[4] although the true costs are difficult to estimate accurately and were likely much higher. Importantly, it set a precedent for the use of cyberspace for coercion to compel another nation to act, and clearly demonstrated how a cyber operation can pose a threat to national security.[5]

The 2015 Christmas attack on the Ukrainian power grid is a second example of coercive cyber power. Power outages were caused by remote cyber intrusions at three regional electric power distribution companies, impacting approximately 225,000 customers.[6] The Ukrainian attack did not happen in a vacuum. Months of targeting and preparatory actions were required to execute the attack. The technical features of the attack included spear phishing to gain access to business networks, the use of the companies' network management tools to further spread and control the attack, changing the underlying firmware in communications devices, erasing the changes that were made by altering the system logs, and conducting a denial-of-service attack on the power company's telephone system to hinder restoral activities.[7]

These 2007 and 2015 attacks are comparable, demonstrating that network-connected systems

3 Stephen Herzog, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses', *Journal of Strategic Security*, Volume 4, Issue 2 (2011): pp. 49-60, https://doi.org/10.5038/1944-0472.4.2.3, 51.
4 Marcin Terlikowski, 'Cyberattacks on Estonia. Implications for International and Polish Security', *The Polish Quarterly of International Affairs*, Volume 16, Issue 3 (2007): pp. 68-87, 75.
5 Rain Ottis, 'Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective', CCDCOE (Cooperative Cyber Defence Centre of Excellence, 2008), https://ccdcoe.org/library/publications/analysisof-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/, 5.
6 The Department of Homeland Security, Cybersecurity and Infrastructure Security Agency CISA, 'ICS Alert (IrAlert-h-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure' (Washington, D.C. July 20, 2021), https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01, 2.
7 Robert M. Lee, Michael J. Assante, and Tim Conway, 'Analysis of the Cyber Attack on the Ukrainian Power Grid', *SANS E-ISAC*, March 16, 2016, 2.

and assets can be held at risk. While there were indications that each attack was Russian state sponsored, it was left to forensic analysis to make this case. Nothing was damaged in the physical sense. This set it apart from the traditional uses of power and posed challenges for national security officials in determining an appropriate response. The inherent right to self-defence exists, but against what target? What should be considered a proportional response? National security decision-making processes were challenged, as well as cyber defences.

Physical destruction has occurred in a handful of cyberattacks. Perhaps the most famous is the June 2010 use of the STUXNET worm to damage Iranian centrifuges that were being used to enrich uranium in pursuit of a nuclear weapon. STUXNET has been attributed to a US / Israeli partnership.[8] STUXNET was another complex cyber event, although the interesting evolution was the relative ease with which the worm spread to other Siemens Programmable Logic Controllers (PLC) worldwide.[9] While there were certainly international tensions over Iran obtaining a nuclear weapon, the attack set a precedent for cyber warfare.

Two years later, perhaps attributable to Iran in retaliation for STUXNET, Saudi Aramco was the victim of the Shamoon malware attack that destroyed 35,000 computers by overwriting the master boot record on their hard drives.[10] In the evolution of cyber events, the Saudi Aramco attack is noteworthy in that it specifically targeted a large company and, like STUXNET, demonstrated the potential to physically destroy equipment. There is a close relationship between Saudi Aramco, the government of Saudi Arabia and, specifically, the nation's petroleum economy. Although the attack didn't hinder oil production, the Saudi economy was at significant risk.

Little has changed from a policy perspective since 2012, which results in imposing costs on either cyber criminals or nations that use cyberattacks in pursuit of international goals. Yet the cost to victims increases with each attack. In 2021, after the discovery of the SolarWinds cyberattack, the 35,000 damaged computers during the Saudi Aramco attack seem small in comparison. SolarWinds is a company that produces IT management software that is used to provide centralized management of a network environment. A program that is normally used to provide software updates and security patches was infected with malware. SolarWinds has reported that as many as 17,000 of its 33,000 customers may have installed the infected software.[11] A list compiled from various news outlets of entities impacted by the SolarWinds breach is extensive, including many governmental entities and Fortune 500 companies. The United States[12] government has attributed this to Russian entities. In the context of cyberattacks, it is unique because of the scale, but also because one cannot readily attribute a motive. Malware delivered via the SolarWinds platform might lie in wait for months or years.

This kind of cyberattack is called a "supply-chain" attack because of the method that it uses to infect networked systems. It is particularly dangerous because the potential number of infected computer hosts is logarithmic. This danger was seen in the breach and subsequent ransomware attack on Kayesa, another US IT company. The Kayesa event demonstrated how quickly a supply chain attack might spread. Within hours of the attack being publicized, a Swedish supermarket chain was forced to close even though it was not a direct Kayesa customer.[13] The costs of cyber breaches continue to rise. A study by the Council of Economic Advisors pegged the cost to the US

8 Ellen Nakashima and Joby Warrick, 'Stuxnet was work of U.S. and Israeli experts, officials say', *The Washington Post*, 2 June, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-workof-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html, 1.
9 Vivian Yeo, 'Stuxnet Infections Spread to 115 Countries', ZDNet, 9 August, 2010, https://www.zdnet.com/article/stuxnet-infections-spread-to-115-countries/, 1.
10 Fahmid Y. Rashid, 'Inside the Aftermath of the Saudi Aramco Breach', Dark Reading, 8 August, 2015, https://www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach, 1.
11 Kevin B Thompson, 'Form 8-K Solarwinds Corp', SolarWinds Corporation, 14 December, 2020, https://sec.report/Document/0001628280-20-017451/, 1.
12 The White House, 'Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government', 15 April, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposingcosts-for-harmful-foreign-activities-by-the-russian-government/, 1.
13 Joe Tidy, 'Swedish coop supermarkets shut due to US ransomware cyber-attack', BBC News, 3 July, 2021, https://www.bbc.com/news/technology-57707530, 1.

economy at between $57 billion and $109 billion in 2016.[14] The range of this estimate reflects the difficulty in assessing actual costs. The costs of restoring services after a cyber breach are often greater than what is required to put IT or control systems back into service. There may also be a loss of revenue and corporate reputation. For example, Equifax, a US credit reporting company experienced a breach in September 2017 that led to the compromise of 140 million personal records. The company's stock price fell by 13% after the breach was announced and ultimately lost more than one-third of its value.[15] Legal costs, reparations to those who experienced data loss, and fines added to the total cost. Direct and indirect costs are estimated to be in excess of 1.5 billion dollars.[16] The costs of cyberattacks are likely to continue to increase despite significant outlays for cybersecurity products and services, a market that grew from 3.5 billion dollars in 2004 to more than 114 billion dollars in 2018.[17]

14 Office of the President of the United States, ed., *The Cost of Malicious Cyber Activity to the U.S. Economy, The Council of Economic Advisers* (Washington, DC, 2018), 2.
15 Ibid., 15.
16 LeeAnne M Pelzer, 'The True Cost of Cybersecurity Incidents: The Problem', Palo Alto Networks Blog, 2 July, 2021, https://www.paloaltonetworks.com/blog/2021/06/the-cost-of-cybersecurity-incidents-the-problem/.
17 Steve Morgan, 'Global Cybersecurity Spending Predicted to Exceed $1 Trillion From 2017-2021', *Cybercrime Magazine*, 10 June, 2019, https://cybersecurityventures.com/cybersecurity-market-report/.

Cyberattacks as a weapon in the hybrid threat arsenal

To control the escalating cyber security costs, many companies turned to cyber insurance to provide financial protection and manage risk in the event of a cyber breach. However, there are aspects of cyber insurance coverage that create national security concerns and make the risk issue murky. NotPetya was a 2017 cyberattack that impacted computer operating systems and, like the Saudi Aramco attack, it rendered computers unusable. NotPetya impacted several global companies, including the Maersk shipping line, the French construction company Saint-Gobain, the Russian oil company Rosneft, and the US drug-maker Merck. The NotPetya attack impacted more than 30,000 computers and 7,500 servers; and it left Merck unable to produce some vaccines. Merck assessed its damages at 870 million dollars and filed a claim with its insurance carriers. The network of insurers that provided cyber insurance rejected that claim on the grounds that the attack was an act of war, an exclusion in Merck's insurance policy.[18]

Although this case has not been settled, it leads to new national security dilemmas. NotPetya has been attributed to the Russian military.[19] While a war had not been declared between Russia and any of the nations where companies were impacted by NotPetya, the insurance carriers equated the involvement by Russia's military with a war-like act. The attribution by the United States (and at least two other nations) did not lead to an overt punitive response.[20] This may cause a criminal group or a nation contemplating a cyber action to believe that the risk of conducting a cyberattack is low. The United States has pursued criminal indictments against both Chinese and Russian hackers who are believed to be affiliated with the military. These actions are largely symbolic as the individuals would need to be extradited to the United States in order for the criminal charges to be acted upon.

Cybersecurity since its inception has been a case of patch and wait – IT and cybersecurity personnel do their best to apply security updates and then wait for an attacker to breach the systems to compromise data or disable systems. Despite the billions spent on anti-virus software and cyber-security monitoring to bolster cyber defence in depth, IT systems are still insecure. The lack of a meaningful reaction to nearly two decades of cyber intrusions and attacks leaves the cyber aspects of the national security environment without an effective deterrent. The potential use of cyber as a means to effect national will or to punish countries that are seen as "out of line" is growing. This does not appear to be moving towards a war between nations, as cyberattacks have not elicited a response using conventional weapons. The danger is that cyber capabilities have been added to the hybrid threat arsenal, thus making hybrid threat actions more complex.

Like other hybrid warfare actions, national security planners must consider cyberattacks when developing response plans at the national level and in dealings with allies. Cyberattacks cannot be ignored, and nor can responses only be the responsibility of cyber-security professionals. A comprehensive framework that demands a timely response to cyberattacks and in a manner that

18 David Voreacos, Katherine Chiglinsky, and Riley Griffin, 'Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?', Bloomberg.com, 3 December, 2019, https://www.bloomberg.com/news/features/2019-1203/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war, 1.
19 The Department of Homeland Security, Cyber and Infrastructure Security Agency, 'Alert CISA, (TA17-181A) Petya Ransomware', 1 July, 2017, https://us-cert.cisa.gov/ncas/alerts/TA17-181A.
20 Cooperative Cyber Defence Centre of Excellence, 'NotPetya', International cyber law: interactive toolkit, 28 June, 2017, https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017).

enhances deterrence against future attacks must be established. Leaders publicly acknowledge the dangers of cyberattacks. NATO General Jens Stoltenberg's admission that "a single cyberattack can inflict billions of dollars' worth of damage to our economies, bring global companies to a standstill, paralyze our critical infrastructure, undermine our democracies and cripple our military capabilities"[21] is one example. But in the moment of a cyberattack, political and military leaders have had difficulty in equating such an attack to a conventional attack. Granted, a response in kind to a cyberattack may be hidden from the public to protect cyber tools. Visible responses, like the creation of the NATO Cyber Operations Centre in Mons help create shared awareness of cyber threats across the Alliance, but have little deterrent effect.

Perhaps this is changing. The NATO summit communiqué that was issued on June 14, 2021, just two days before the meeting between US President Joseph Biden and Russian President Vladimir Putin, reaffirmed that Article 5 could be invoked in response to a cyberattack. More promising is the commitment to "make greater use of NATO as a platform for political consultation among Allies, sharing concerns about malicious cyber activities, and exchanging national approaches and responses, as well as considering possible collective responses. If necessary, we will impose costs on those who harm us. Our response need not be restricted to the cyber domain".[22]

The timing is important. On June 16, 2021 Biden and Putin held their first meeting. Biden warned Putin that attacks on US critical infrastructure would be met with a US response. The test of issuing such a warning is that it must be matched with a willingness to provide public attribution for cyberattacks, and the United States must follow up in this area. Not knowing where a cyberattack came from or being unwilling to disclose a source restricts the available options and mutes a meaningful international response. Not responding to a cyber event or perhaps acting in a manner that is not attributable has limited deterrent value. Additionally, a significant part of the 'grey' area is understanding where cybercrime stops, and state activity begins. It is widely assumed that Russia, China, North Korea, and Iran each turn a blind eye and allow criminal organizations to carry out criminal activities such as ransomware attacks and outright theft using cyber exploits.[23] There is early evidence that this may work. In July 2021, the US called out China for conducting an attack on Microsoft's exchange server. Within a week, NATO, the European Union, and several allies joined the United States in condemning the attacks.[24]

The US warning is extremely broad in scope. The red line that President Biden drew is based upon Presidential Policy Directive 21 (PPD-21), which defines the 16 Critical Infrastructure Security sectors.[25] Although these sectors are what governments would be expected to protect, the PPD-21 list is expansive, perhaps overly so. It may have made more sense to be purposely ambiguous and state that a cyberattack would be met with a response. The challenge for nations is to define cyber centres of gravity in a manner that is sufficiently specific, and where mutual support between government and industry can be achieved.

21 Jens Stoltenberg, 'NATO Will Defend Itself', *Prospect*, October 2019, p. 4.
22 NATO, 'Brussels Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 14 June 2021', 14 June, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm, no 32.
23 Some of this is circumstantial. Ransomware employed by Russian attackers routinely check for the presence of a Cyrillic keyboard. This prevents an exploit being used against a domestic Russian target. Another example are the criminal indictments by the United States of Chinese military personnel engaged in criminal hacking activities. Lastly, state-sponsored hackers from North Korea are believed to use criminal activities to garner much-needed fiscal resources to fund government programmes.
24 'After Failing to Dissuade Cyber-Attacks, America Looks to Its Friends for Help', *The Economist*, 24 July, 2021, https://www.economist.com/united-states/2021/07/20/america-and-its-allies-admonish-but-do-not-punish-china-for-hacking, 1.
25 The Department of Homeland Security, 'Critical Infrastructure Sectors', (Cybersecurity and Infrastructure Security Agency CISA, 21 October, 2020), https://www.cisa.gov/critical-infrastructure-sectors. The 16 critical sectors are: Chemical Sector; Commercial Facilities Sector; Communications Sector; Critical Manufacturing Sector; Dams Sector; Defense Industrial Base Sector; Emergency Services Sector; Energy Sector; Financial Services Sector; Food and Agriculture Sector; Government Facilities Sector; Healthcare and Public Health Sector; Information Technology Sector; Nuclear Reactors, Materials, and Waste Sector; Transportation Systems Sector; and Water and Wastewater Systems Sector.

Measures to consider

The commercial aspect of cybersecurity is critical. For the most part, the commercial sector owns the internet and the networked assets that can be held at risk. In issuing a warning, there is an assumption that a government or a commercial provider can provide adequate warning for the sector that is at risk. The individual sectors themselves have not, historically, provided adequate cyber defence in any of these areas, including information technology. Across the PPD-21 sectors, network systems are often intertwined and at different levels. For example, the food and agriculture sector supply chain is connected to the retail grocery sector. Going beyond that, the significant use of information technologies for financial, supply chain, and service to customers means that an exploit that is used in one area of a business may affect adjacent areas in ways that are not predictable. Amid the ambiguity and the fragmented cyber defence, roles must be defined for red lines to have an effect.

The approach to cybersecurity and the defence of networks must improve. Cybersecurity is overdependent on individual users. It is complicated both by the vastness of the internet and the lack of personal responsibility at the enterprise level. Principles for "secure by default" with systems that are secure regardless of an individual's actions should be the standard for new systems.[26] For networks and systems, zero trust principles requiring all system users to be authenticated should be implemented.

Since the mid-2000s, nearly 40 countries have created military-affiliated cyber forces.[27] In the years that have followed there has been organizational activity designed to integrate the cyber forces into military service structures, the establishment of equipment programmes, as well as training and exercises that complement the introduction of these military units. White papers and national cyber strategies have emerged that are designed to set agendas and priorities. Still, operating in cyberspace remains a shadowy area that lacks a tested policy and doctrine that would allow military cyber forces to function optimally in support of a nation's security objectives.

One doctrinal concept that has emerged is the idea of "defending forward", which was articulated by the head of US Cyber Command, General Paul Nakasone, in the summer of 2020. "Defending forward" leverages the notion of persistent engagement and extends the operational boundaries. Cyber Command believes that "this more proactive approach enables Cyber Command to conduct operations that impose costs while responsibly managing escalation".[28] Restated, what General Nakasone is saying is that to properly defend cyberspace it is necessary to operate inside the networks of those nations that present a direct threat to US networks. While the idea of persistent engagement is not a new one for national security, for cyber forces it is an admission that traditional cyber defences such as passwords, firewalls, monitoring and patching security bugs in software are not in themselves sufficient for a robust cyber defence. Cold War air defence is analogous. It was commonplace to closely track, intercept and escort Russian aircraft operating in proximity to NATO borders. The North American Aerospace Defense Command (NORAD), a combined US / Canada command, continues these practices in the northern latitudes today. As "defending forward" matures as an operational construct, it could provide a viable deterrent and help prevent cyberattacks.

26 A detailed technical explanation for secure by default can be found at https://www.ncsc.gov.uk/information/secure-default.
27 Jason Blessing, 'The Global Spread of Cyber Forces, 2000–2018' (NATO Cooperative Cyber Defence Centre of Excellence, 2021), https://ccdcoe.org/uploads/2021/05/CyCon_2021_Blessing.pdf.
28 Paul M. Nakasone and Michael Sulmeyer, 'How to Compete in Cyberspace', *Foreign Affairs*, 25 August, 2020, https://www.foreignaffairs.com/print/node/1126408, 7.

Conclusions

The precedents of cyberattacks over the last 15 years impact both those who carried out the intrusions and those who attempt to defend networks. The current cybersecurity environment indeed resembles the punishment of "death by a thousand cuts". It is extraordinarily expensive and damaging. Small and large intrusions become footholds for later attacks or a proving ground for the development of cyber weapons. Leaders across all government and commercial sectors, as well as the cybersecurity professionals trusted to protect connected systems, have been conditioned by the relentless stream of cyber intrusions, crimes, and attacks to think that these attacks are normal. It is to the advantage of cyber criminals and states employing cyberattacks to maintain the status quo. Both traditional cybersecurity methods and the way in which nations respond to intrusions and attack must evolve.

As the commercial IT sector owns much of the internet environment, government and business leaders will have to collaborate in order to manage the risk to both public safety and investments. This suggests an evolving policy framework that encompasses both proactive and reactive responses to cyber threats. The operational doctrine employed by national cyber forces and by national security alliances must be developed, tested and matured. The bilateral exercises that have been developed are a great first step. The next phase should be to include industry partners in the exercises. This will be part of the long-term cybersecurity solution and governments must not be afraid to let industry cyber experts take the lead.

Lastly, the global nature of the internet demands international cooperation. Individual nations have varying legal authorities to respond to cyber events. Collectively, these authorities provide NATO with significant flexibility to respond to cyber threats. Although methods will differ, consistency in the tenor of the response to cyber intrusions and attacks is needed. NATO has decades of experience in developing political and operational options for conventional threats. Now is the time to apply this expertise to address the long-term cyber-security concerns.

Author

Rear Admiral (retired) William Leigher served in the United States Navy for 33 years in intelligence and cryptologic warfare. His Navy assignments included serving as the Deputy Director for Information Technology and Communications at Commander, Naval Security Group Command, Fort Meade, Maryland and at the National Security Agency, where he served as a Senior Operations Officer in the National Security Operations Center. He also served as the Commanding Officer Naval Information Operations Command in Norfolk, Va., where he was selected to flag rank in 2008. As a Flag Officer, he focused on cyber warfare, serving as the Director of Information Operations on the staff of the Chief of Naval Operations, as the Deputy Commander for US Fleet Cyber Command/US 10th Fleet, and the Director of Warfare Integration for Information Dominance on the Navy Staff in the Pentagon. He retired from the Navy in 2014 and worked in the defence industry, focusing on developing cyber capabilities for the military.


Hybrid CoE