Between Two Stools: Military and Intelligence Organizations *in the Conduct of Offensive Cyber Operations*

Ewan Lawson

From 2018, members of the coalition fighting against the Islamic State in Iraq and Syria confirmed that they had been conducting offensive cyber activities as part of the campaign in an operation given the codename GLOWING SYMPHONY.[1] While the details of these operations largely remain highly classified, they are the first example of states publicly admitting to such operations during armed conflict. They are also notable as while Fleming in his speech cited above emphasized that the UK effort resulted from cooperation between its signals intelligence (SIGINT) agency GCHQ and the Ministry of Defence (MOD), one of the other partners, Australia, emphasized the role of civilian personnel from its SIGINT organization, the Australian Signals Directorate.[2] This was arguably the first public recognition of the extent to which, at least in some states, intelligence organizations and the military were entwined in the conduct of contemporary offensive cyber operations.

This integration is likely to be a feature of future offensive cyber operations. In October 2021, it was revealed that the UK's National Cyber Force (NCF), which includes intelligence officers, military personnel, and law enforcement, was conducting such operations against actors involved in a series of ransomware attacks, providing further evidence of a blurring of the actors involved in offensive activities in cyberspace.[3]

While it is recognized that this is taking place partly in response to some states deliberately making use of organized crime groups or civilian so-called: patriotic hackers, this article argues that the blurring of responsibilities between intelligence agencies and the

Ewan Lawson is an independent researcher on defence and security issues having previously been a Senior Research Fellow at the Royal United Services Institute. He is also a Teaching Fellow at the School of Oriental and African Studies at the University of London and has been engaged by the International Committee of the Red Cross, to examine military cyber operations and international humanitarian law.

He researches a range of subjects including cyber security, strategy and cross-government working, military influence and information operations, law of armed conflict and war crimes, and conflict in Africa.

He was previously a Royal Air Force officer, completing joint warfare appointments including tours as a joint operational planner, as the commander of the UK Psychological Operations Group, as faculty at both the UK and Kuwait Staff Colleges and as Defence Attaché in South Sudan. He also worked on the development of UK cyber warfare capabilities.

military in the conduct of offensive cyber operations is problematic and that there is a need for deliberate organizational and operational distinction. What is, in effect, the para-militarization of operations in cyberspace has the clear potential to contribute to instability in the international system in two main ways. First, it contributes to the risk of unexpected and unintended escalation through reinforcing the security dilemma for states subject to hostile intrusions. Second, it contributes to the growing space for disruptive and destructive operations below the level of armed conflict in the so-called "grey zone," and hence outside the spaces where civilians can be protected under international humanitarian law (IHL).

The article first outlines the background of how this position has arisen. In doing so, it will focus on the states that declared their involvement in GLOWING SYMPHONY: the UK, Australia, and the US as cases. Having considered the organizational context, it then reviews whether there is something inherent in cyberspace that leads to what has been called an intelligence competition.[4] It next moves on to consider how the blurring of responsibilities in military cyber operations between intelligence organizations and the military might increase the risk of unforeseen escalation, and the implications of operations conducted below the level of armed conflict. Finally, it considers how states might address this issue.

In many states, intelligence agencies play a significant role in building capacity in both cyber security and offensive cyber operations. This reflects in part that those agencies have transitioned from traditional signals intelligence to also collecting data from digital sources. They have developed access to the networks of actual and potential adversaries, primarily for the purpose of intelligence collection but increasingly with an awareness of the potential to deliver both physical and cognitive effects through the addition, deletion, or manipulation of data on those networks.

As militaries became aware of this potential to deliver destructive or disruptive effects through offensive cyber activities during the conduct of operations, an inevitable linkage with the intelligence agencies in this field developed. Indeed, in some cases the signals intelligence agencies had their roots in, or indeed still were part of, the military. In the UK, GCHQ as the national SIGINT agency has taken the technical and operational lead in many aspects of cyber policy and formed the base around which the National Cyber Security Centre (NCSC) was established in 2016 as the focus for cyber security and national cyber defense.[5]

Over the last decade, the UK has reorganized its offensive cyber capabilities, culminating in the formation of the NCF in 2020. This seeks to bring together the operational experience of GCHQ and MOD along with the overseas-focused Secret Intelligence Service (SIS) and the research organization Defence, Science and Technology Laboratories (Dstl).[6] It builds upon a longer relationship between the military and GCHQ in SIGINT and a developing one in the conduct of offensive cyber operations. It is important to note that from its launch the NCF has been expected to operate against a range of targets, not just states and violent non-state actors but also criminal groups.[7]

Whereas in the UK, GCHQ reports to the Foreign, Commonwealth and Development Office (FCDO), the Australian Signals Directorate (ASD) has retained its roots as a statutory agency within Defence since 2017. Similarly, the US SIGINT elements, the National Security Agency (NSA), operates under the Department of Defense although its Director is "dual-hatted" as the military commander of U.S. Cyber Command (USCYBERCOM). This latter organization delivers cyber support, both offensive and defensive, to US military operations, although the regional combatant commanders that cover the globe also have cyber capabilities under their command.

It is important to recognize that many states' intelligence agencies have a paramilitary aspect to their operations. In the examples of the UK and Australia, these sorts of activities are usually conducted by military personnel acting in support of the civil power. In the US, the Central Intelligence Agency (CIA) has had a paramilitary component since being formed at the end of World War II as the successor to the Office of Strategic Services (OSS).[8] The most visible contemporary manifestation of this is the undeclared campaign of targeted killings undertaken by drones as part of counterterrorism operations in places like Pakistan, Somalia, and Yemen. Although authors have questioned the extent to which these operations are compatible with domestic and international law, it seems likely that the use of paramilitary forces in conflicts that fall below the threshold of armed conflict will be part of future inter-state competition including in cyberspace.[9] This is already seen in USCYBERCOM's strategic approach of persistent engagement which will be discussed later in this article.

As noted previously, it is important to recognize that this blurring of organizations involved in delivering effects in cyberspace is not unique to Western democracies. Indeed, the desire to respond to coercive activities conducted by adversaries and competitors in cyberspace below

the level of armed conflict is a significant driver in the development of these approaches. The relative anonymity provided by cyberspace has encouraged states to take the opportunity this provides to operationalize coercive strategies using actors including organized crime groups and "patriotic hackers" with the intention of distancing the state from the activity. The blurring described here between intelligence and military organizations is arguably less morally, ethically, and legally contentious but, as will be outlined, it has potentially similar impacts in terms of escalation risk and undermining IHL.

It can be seen that, at least in the three Western examples, the national structures designed to deliver offensive cyber capability involve a mix of civilian and military personnel, and capabilities from intelligence agencies and the military. At the heart of this combination is the challenge of gaining access to networks and systems whether for the purposes of gathering intelligence or delivering effects. This is an essential step in either form of operation and, indeed, reconnaissance of a target system is part of any offensive cyber "kill chain" process.[10] Given that the priority in the early stages of the digital revolution was on the opportunities for accessing and exploiting data, it is unsurprising that the intelligence agencies developed the skills necessary for identifying and exploiting such accesses.

Conceptually, academics and commentators frequently question whether traditional frameworks to describe war and conflict are appropriate when applied to cyberspace. One alternate framework recognizes the central role of intelligence agencies and suggests that it is better described as an intelligence contest.[11] At its heart, an intelligence contest is about stealing information from competitors and adversaries, protecting one's own information, and disrupting the opponent's data and communications. Rovner identifies five defining characteristics of an intelligence contest:[12]

a. An effort to collect more and better information on adversaries' capabilities and intentions.

b. An effort to exploit any discovered information for practical gain such as decision advantage or to improve the balance of capabilities.

c. An effort to undermine adversary morale, institutions, and alliances.

d. An effort to disable adversary intelligence collection capabilities.

e. A campaign to pre-position assets for future collection including in the event of armed conflict.

On this basis, Rovner argues that current competition in cyberspace is more reflective of an intelligence contest than being framed through the language of war and armed conflict.[13] On this basis, the central role for intelligence agencies in cyber operations seems logical. However, even Rovner recognizes that it does not quite cover the extent of offensive cyber operations, which also include military conflict and some forms of diplomacy.[14]

Critiques of this alternate way of conceptualizing conflict in cyberspace note both the kinship between intelligence operations and those in cyberspace, including covert paramilitary actions. However, rather than seeing intelligence operations as the central activity in cyberspace, instead note they are conducted in support of diplomacy, military operations, and internal security.[15] In particular, Warner argues that Rovner's five characteristics are representative of cyber operations in support of diplomacy and internal security but not military operations which are likely to be more destructive than merely disruptive.[16] While some would argue that the use of military language with regard to cyberspace operations is simply a way of achieving bureaucratic and budgetary advantage, the critique highlights the limitations of focusing on the intelligence contest approach.[17] This in turn highlights the potential for problems with the blurring of operations conducted by intelligence organizations as part of the contest and those conducted by the military as part of an armed conflict. But in what ways might those problems manifest in practice?

One of the key challenges links to the condition of uncertainty that exists in international politics.[18] In the international relations theory of defensive structural realism, the nature of the international system can give rise to the security dilemma. Defensive structural realists see states acting to secure themselves in an anarchic international system. It argues that states are fundamentally rational, and that conquest or military aggression is difficult given that the balance is in favor of the defense. It therefore argues that states should rationally seek to maintain the status quo and hence seek to balance against competitors.[19] While this theoretical framework can be effective at explaining response to coercive or aggressive activities by a state, it is less useful in explaining why states might choose those approaches. One possible explanation is the security dilemma in which states undertake policies designed to secure their own security, which either by design or unintentionally reduce the security of an adversary or at least its perception of security. In turn, the adversary may react to this perception by adopting policies that in turn decrease the security of the originator. In this way, conflicts can escalate, whatever the original intentions.[20] Ultimately, this is a dilemma of interpretation as well as a dilemma of response.[21]

Buchanan makes a compelling case for the applicability of the security dilemma to states' interactions in cyberspace.[22] In particular, he notes that operations which seek to collect information and gain intelligence, however conducted, can be threatening to the states against which they are conducted.[23] It does not matter if the intentions of the collecting state are relatively benign; it is the perception of the target that is key, along with the decision as to what is an appropriate response. Thus, in the Cold War, NATO aircraft flew toward the borders of the Warsaw Pact in order to collect both technical intelligence on radar systems but also on the nature of the response. Although this activity had an intent that was simply about collecting information, it ran the risk of being misinterpreted as part of an aggressive strike.

In cyberspace, the problem arises in the first instance when a defender detects that an actor has gained access to its network. While most computer network exploitation operations will be designed to go undetected, this clearly cannot be guaranteed, and to the target it is likely that it will at least initially be unclear as to the precise purpose of the intrusion. Thus, there is a clear risk of misperception potentially influenced by the wider political and security context at the time. Through technical analysis and the identification of patterns of use of tools, techniques, and infrastructure, it is possible to identify threat actors and link them to organizations including intelligence agencies, albeit with varying degrees of certainty. A target may be able therefore to make some deductions as to the purpose of the intrusion based on the identity of the threat actor.

The integration of intelligence agencies with the military in the conduct of offensive cyber operations could therefore easily lead to the misperception that an intrusion, conducted by the former for the purposes of exploitation, could be for disruptive or destructive purposes as part of a military campaign. Would this in and of itself necessarily be escalatory? It has been argued that "past cyber incidents are associated with limited escalation,"[24] but the evidence base is at present limited. It appears that escalation arising from competition and conflict in cyberspace may be more complex than the traditional model of a ladder or spiral. Given that the "linkages between intent, effect and perception are loose,"[25] it is possible that escalation may be as much horizontal, into other domains, as vertical and increasing the intensity of the conflict in cyberspace.[26] While the risk and indeed the nature of escalation arising from operations in cyberspace continue to not to be well understood and, given the limited evidence base to date, it would seem sensible to minimize that risk wherever possible, including reducing the risk of misinterpretation of the purpose of such operations.

One way in which some states perhaps have sought to minimize the risk of escalation is through coercive activities which are designed to stay below the level of a conventional military response. This so-called "hybrid warfare" has been enabled by the digital revolution and has included disruptive offensive cyber operations and digitally-enabled information operations. The continuing conflict in Ukraine has seen disruption of the power grid in Kyiv along with disinformation campaigns targeted at the population both in Ukraine itself and in friendly states.[27] It has also included cyber operations against military targets and a domestically developed app which improved the targeting of Ukrainian artillery but was hacked in order to provide location data that in turn allowed those formations to be attacked.[28] While it can be argued that hybrid activities taking place in Donbas are part of an armed conflict and therefore need to be conducted in accordance with the principles of IHL, it is less clear that an offensive cyber operation in Kyiv reaches that threshold.*

The principles of IHL are designed to protect non-combatants during armed conflict, and states have broadly agreed at the UN that these apply to operations in cyberspace.[29] However, the International Committee of the Red Cross (ICRC) in a recent report raised concern

*This article was written before the implications of the Russian invasion of Ukraine in February 2022 could be evaluated and hence refers to the period of conflict before that.

that states may have differing perspectives on the applicability of IHL to offensive cyber operations conducted in the context of hybrid warfare below the threshold of armed conflict.[30] While some have indicated that they would apply the principles of IHL to all offensive cyber operations which might impact civilians, this is far from universally agreed and remains a contentious issue. To an extent, the debate focuses on technical legal arguments around what constitutes an "attack" as defined in the Geneva Conventions when conducted in cyberspace, and whether "data" can be considered an object under IHL. However, it also reflects the broader discussion about operations conducted below the legal threshold of armed conflict and the need to protect civilians.[31]

Further, the ICRC report also raises concern about the role of intelligence agencies in the conduct of offensive cyber operations, noting that the authorities for conducting espionage or exploitation are in many states different from those enabling disruptive and destructive effects. Further, the report highlighted that the international norms and laws for managing armed conflict are considerably more developed than those for espionage. This raises concerns about how cyber operations that transit from exploitation to an offensive function are managed, particularly when it involves a transition of responsibility between an intelligence agency and the military.[32]

The current posture adopted by USCYBERCOM also blurs this line between intelligence collection and disruptive/destructive offensive cyber operations. DoD adopted a strategy known as "Defend Forward" which has been operationalized by USCYBERCOM through the doctrine of "Persistent Engagement".[33] The intent is to identify, counter, and mitigate threats before they enter US networks or impact US interests. This requires the aggressive collection of intelligence which, coupled with the potential for such accesses to be developed into offensive cyber operations, raises again the risk of escalation through misinterpretation and the security dilemma. While this approach is designed to counter the potentially corrosive effects of activities such as election interference and is apparently conducted under appropriate national authorities and cognizant of international law, it once again blurs the distinction between intelligence operations and those designed to deliver effects, and are conducted by a military organization potentially below the threshold of armed conflict. Further, it has been argued that if Persistent Engagement is the focus of USCYBERCOM it risks a mindset that prioritizes aggressive tactics which might be appropriate in a period of relative peace when escalation is unlikely but might be counterproductive in a period of intense crisis or conflict. If these are the risks from the blurring of intelligence agencies and the military in cyberspace, what are the options?

This article does not seek to argue that states should not respond to coercive and aggressive activities in cyberspace. Indeed, it can be argued that although each has a different construct the approaches adopted in Australia, the UK, and the US in creating hybrid organizations balances the risk of blurring the legal frameworks for those cyber operations designed for exploitation and those for effect. While inevitably the detail of how they operate is opaque, there

is little doubt about the potential to ensure shared understandings across the organizations of responsibilities and authorities, and to manage the transitions between intelligence collection and effects operations in ways that minimize the risks of those responsibilities and authorities being misunderstood or misused. However, as this article argues, it also contributes to increasing the risk of misperception on the part of the target as to what is intended, which could in turn have unforeseen escalatory consequences. Therefore, what is the alternative?

States should consider how they create clear structural and practical distance between those organizations tasked with intelligence collection, and network exploitation for that purpose, and those that are tasked with delivering disruptive and destructive effects, whether cognitive or physical. This would contribute to reducing the risk of misperceptions as to the reasons behind a network intrusion when it is discovered by a target state and the initiating organization is identified or suspected. More research is required into the relationships between perceptions and escalation risk resulting from cyber operations, and the relative significance of factors such as the political context, the nature of the targeted system, and the potential identification of the type of organization conducting the operation. This research could be conducted through the analysis of real-world case studies as well as tabletop exercises conducted with practitioners.

In this way, an organization such as the NCF in the UK, while attractive in terms of potential operational and fiscal efficiencies, contributes to increasing the risk. Equally, given the continuing intensity of competition and conflict in cyberspace, it would be naïve to expect a successful cyber power not to seek to exploit and develop opportunities identified through intelligence operations. Therefore, there is a need to consider alternate organization models. For example, rather than creating an integrated organization, another approach would be to create a central coordination mechanism that would allow those organizations which need to conduct operations in cyberspace, whether for exploitation or to deliver effects, to focus on their areas of responsibility while ensuring that opportunities identified by agencies are not missed by others. This will, of course, always leave the debate in certain circumstances as to whether delivering an effect and hence potentially losing access and valuable intelligence is the right decision, but these options are ones that are best addressed by an organization that is separate from the bureaucratic interests of the various operators. It can make operational decisions based on a clear understanding of national strategy.

The US has had a more public discussion of some of these issues resulting in part from the leaks of material by Edward Snowden but also a complex interagency process which some have argued has impacted the ability of USCYBERCOM to respond to hostile cyber operations in a timely manner. These issues appear to have been addressed through the allocation of greater authority to the military, but it is not clear that this will reduce the risks highlighted in this article, and indeed it might intensify them.[34]

In conclusion, the blurring of actors in cyberspace continues to be a concern, whether referring to those states using non-state actors such as organized crime groups or "patriotic hackers," or those such as Australia, the UK, and the US, which have sought to integrate military and civilian intelligence capabilities. While the latter is arguably necessary given the challenge of coercive activities in cyberspace and the benefits that would accrue from operational and fiscal efficiency, this article argues that it adds to the potential risks arising from this blurring.

In particular, the nature of cyberspace means that for states targeted it can be difficult to assess the purpose of an intrusion. This creates a potential security dilemma for those on the receiving end in terms of both perception and response. Although escalation risk from activities in cyberspace is still not well understood, the continuing integration of organizations with responsibility for exploitation and the delivery of effects increases the risk of misperception and unintended escalation. Further, offensive cyber operations below the level of armed conflict may not be conducted under the principles of IHL but potentially under legal frameworks designed for intelligence collection and exploitation. This potentially contributes to an increased risk of civilian harm arising from offensive cyber operations.

Future offensive cyber activities have the potential to be more disruptive and indeed destructive. While some states (often disingenuously) have called for the demilitarization of cyberspace or its being maintained as a venue for peaceful activities only, the offensive cyber genie is already out of the bottle. Instead, we should actively consider the extent to which contemporary thinking on offensive cyber is contributing to future risks; both to international peace and to our societies. Consideration needs to be given to whether the integration of intelligence and military cyber capabilities is the best approach in light of the risks and whether instead there is a need to create clear space between the different organizations within a state that have a legitimate reason to operate in cyberspace. The risks of unintended escalation and of civilian harm should outweigh the desire for perceived operational and fiscal efficiency.

NOTES

1. Jeremy Fleming, 2019, Speech at *Cyber UK 2018*, GCHQ, https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018.
2. Stephanie Borys, 2019 *Licence to Hack: Using a Keyboard to fight Islamic State*, ABC News Online, https://www.abc.net.au/news/2019-12-18/inside-the-islamic-state-hack-that-crippled-the-terror-group/11792958?nw=0&r=HtmlFragment.
3. Helen Warrell, 2021, "GCHQ to use new cyberforce to hunt ransomware gangs," *Financial Times,* https://www.ft.com/content/2e391872-428d-44bf-8910-23f123c8aaa6, accessed October 28, 2021.
4. Robert Chesney and Max Smeets, 2020, "Introduction: Is Cyber Conflict an Intelligence Contest" in: P*olicy Roundtable: Cyber Conflict as an Intelligence Contest.* Austin: Texas National Security Review, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.
5. NCSC. n.d. *About the NCSC: What we do*, https://www.ncsc.gov.uk/section/about-ncsc/what-we-do, accessed September 13, 2021.
6. Joe Devanny, Andrew Dwyer, Amy Ertan, and Tim Stevens 2021, *The National Cyber Force that Britain Needs?* London: Kings College London, 7.
7. NCSC n.d.
8. D.H. Berger, 1995, *Use of Covert Paramilitary Activity as a Policy Tool: An analysis of Operations conducted by the US Central Intelligence Agency*, 1949-51, United States: Marine Corps Command and Staff College, https://www.hsdl.org/?abstract&did=445885.
9. Sterio, Milena. 2018. "Lethal Use of Drones: When the Executive is Judge, Jury and Executioner," *The Independent Review*, Vol. 23 No. 1, 35-50.
10. Christopher Whyte and Brian Mazanec, 2019, *Understanding Cyber Warfare: Politics, Policy and Strategy*, London: Routledge, 93.
11. Chesney and Smeets, 2020.
12. Joshua Rovner, 2020, "What is an Intelligence Contest?" in: Policy Roundtable: Cyber Conflict as an Intelligence Contest, Austin: Texas National Security Review. https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.
13. Ibid.
14. Ibid.
15. Michael Warner, 2020, "The Character of Cyber Conflict" in Policy Roundtable: Cyber Conflict as an Intelligence Contest, Austin: *Texas National Security Review*, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/,
16. Ibid.
17. Jon R. Lindsay, 2020, "Military Organisations, Intelligence Operations and Information Technology" in: Policy Roundtable: Cyber Conflict as an Intelligence Contest, Austin: *Texas National Security Review*, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.
18. Ken Booth and Nicholas J. Wheeler, 2018, "Uncertainty," in Paul D. Williams and Matt McDonald (eds.), *Security Studies: An Introduction 3rd Edition*, Abingdon, UK: Routledge, 132.
19. Michael A. Jensen and Colin Elman, 2018, "Realisms," In Paul D. Williams and Matt McDonald (eds.), Security Studies: An Introduction 3rd Edition. Abingdon: Routledge, 23
20. Charles L. Glaser, 2013, "Realism," In *Contemporary Security Studies* (3rd Edition), edited by Alan Collins, 13-27, Oxford: Oxford University Press, 16.
21. Booth and Wheeler 2018, 133.
22. Ben Buchanan, 2016, *The Cybersecurity Dilemma: Hacking Trust and Fear between Nations. London: Hurst and Company.*
23. Ibid., 23.
24. Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, 2018, *Cyber Strategy: The Evolving Character of Power and Coercion*, Oxford: Oxford University Press.
25. Martin C. Libicki, 2012, *Crisis and Escalation in Cyberspace*, Santa Monica: RAND Corporation, xvi.

NOTES

26. Martin C. Libicki and Olesya Tkacheva, 2020, "Cyberspace Escalation: Ladders or Lattices?"In A. Ertan, K. Floyd, P. Pernik, and T. Stevens (eds.), *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Tallinn, Estonia: NATO CCD COE, 62.
27. CIVIC, 2021, *Entering the Grey Zone: Hybrid Warfare and the Protection of Civilians in Ukraine*, https://civiliansinconflict.org/publications/policy/entering-the-grey-zone/, 17.
28. Adam Meyers, 2016, *Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units,* Crowdstrike Blog, https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.
29. UN GGE, 2021, *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security*, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf, 14.
30. ICRC, 2021, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflict*, Geneva: ICRC, 14.
31. Michael Schmitt, 2021, *The Sixth United Nations GGE and International Law in Cyberspace*, Just Security Blog, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.
32. ICRC 2021, 15.
33. Paul M. Naksone and Michael Sulmeyer, 2020, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs*, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.
34. Robert Chesney, 2018, *Offensive Cyber Operations and the Interagency Process: What's at Stake with the New Trump Policy*, Lawfare Blog, https://www.lawfareblog.com/offensive-cyber-operations-and-interagency-process-whats-stake-new-trump-policy.