Chapter 5

Will Cyber Autonomy Undercut Democratic Accountability?

Ashley Deeks[1]

I
INTRODUCTION

In recent years, democratic legislatures have struggled to maintain a role for themselves in government decisions to conduct extraterritorial military operations, including those that involve the use of force. The US Congress offers a prime example of this phenomenon, but other legislatures such as the British Parliament and the French National Assembly face similar challenges.[2] Some of these challenges are due to constitutional provisions, institutional structures and historical practice. Even

1 Thanks to Kristen Eichensehr, Duncan Hollis, John Hursh, Chris Spirito, Paul Stephan, and participants in the NATO CCDCOE group that is examining the legal implications of cyber autonomy for very helpful comments and conversations, and to Ben Doherty and Christopher Kent for outstanding research.

2 See, eg, *United Kingdom, House of Commons, Public Administration and Constitutional Affairs Committee, 'The Role of Parliament in the UK Constitution: Authorizing the Use of Military Force'* (6 August 2019) <https://publications.parliament.uk/pa/cm201719/cmselect/cmpubadm/1891/189102.htm>; Delphine Deschaux-Dutard, 'Parliamentary Scrutiny of Military Operations in France and Germany' (European Consortium for Political Research) <https://ecpr.eu/filestore/paperproposal/ca1d8496-d41c-47d7-96c7-d35ef4532c90.pdf> accessed 14 October 2020. Although legislatures in non-democratic systems also face challenges in regulating and overseeing their executives, that problem extends far beyond the cyber issues that I discuss here.

constitutions that give legislatures a role in authorizing military force *ex ante* often empower executives to respond to sudden attacks without legislative blessing. Further, executive branches are necessarily better structured than legislatures to collect classified information, respond quickly to urgent security threats and direct military operations.[3]

Not all legislative limitations are linked to constitutional rules or structures, however. These legislatures are also struggling to preserve their roles because of the changing nature of conflict: a shift away from large-scale, kinetic operations toward smaller-scale operations, including operations in cyberspace, that are harder to detect publicly and do not require the type of robust legislative support that large-scale conflicts do.[4] These modern operations leave legislatures struggling to learn the facts and engaging in *ex post* and sometimes ineffective efforts to hold their executive branches accountable for offensive cyber operations that could lead to hostilities with other States.

The introduction of increased autonomy into this setting has the potential to further alter the existing relationships between executives and legislatures in making decisions that implicate the use of force. Because the use of autonomous cyber tools may lead States into serious tensions — if not armed conflict — with other States without advance notice, these capabilities pose particular hurdles for legislatures that already struggle to stay relevant on use of force and cyber issues. Additionally, a State's ability to employ autonomous cyber tools may alter the dynamics among different actors *within* executive branches themselves — by, for instance, diverting deliberative input and oversight abilities away from foreign, intelligence and justice ministries and toward defense ministries in the lead-up to conflict.

This article explores how the use of increasingly autonomous cyber tools may alter the current state of legislative oversight and internal executive decision-making about the resort to force. It also illustrates how these changes may impact international peace and security; and it identifies ways in which States may prevent a further erosion of democratic accountability for cyber-related *jus ad bellum* decisions. Unless legislatures take steps now to preserve a role for themselves, and unless executive

3 Overclassification by executive branches, or an excessive unwillingness to share classified information with legislative overseers, are persistent problems in checking executive national security activities. This article assumes that legislatures will continue to face hurdles on this front, and intends to highlight how cyber autonomy will create additional hurdles.

4 Jack Goldsmith and Matthew Waxman, 'The Legal Legacy of Light-Footprint Warfare' (2016) 37 The Washington Quarterly 7, 10 (noting that cyberattacks are low-visibility and arguing that they 'attract[] less public, congressional, and diplomatic scrutiny than the operations [they] replaced').

branches ensure that an appropriate diversity of officials remains involved in use of force decisions, key vestiges of democratic accountability for those decisions may fall away. Executives will not wait long for their legislatures to act, given the urgency of cyber threats.

Part II examines the likely trajectory of national security-related cyber autonomy within various States. Part III briefly sets out the powers that various States have allocated to their legislatures on use of force issues. Part IV synthesizes those analyses to contemplate the additional challenges that growing levels of cyber autonomy will pose to legislatures — and civilian actors within executive branches — that seek to retain input into governmental decisions that may lead to interstate conflict. Part V sets out some normative proposals for ways in which legislatures and executive branches can meet these challenges. This Part argues that legislatures should bolster their own technological expertise and consider enacting laws that place appropriate parameters on the executive branches' development and use of cyber autonomy. Within executive branches, civilian policymakers and lawyers from a range of agencies should insist on a role for themselves in developing the rules of the road for using autonomous cyber tools.

II
THE PROSPECTS FOR CYBER AUTONOMY

In national security settings, States are increasingly likely today to deploy cyber tools that use heightened levels of autonomy. This Part describes generally the prospects for burgeoning cyber autonomy within State military and intelligence systems, and then details the ways in which cyber autonomy may lead to situations of serious interstate tensions or even armed conflict.

A DEFINING CYBER AUTONOMY

Before discussing why States have incentives to increase the levels of autonomy that they build into their cyber tools, it is necessary to explain what this article means by 'autonomy'. Autonomy exists on a continuum:

systems may be more or less autonomous, or not autonomous at all.[5] As Tim McFarland writes:

> While there is no precise threshold [beyond which a system becomes autonomous], the term is generally associated with self-governing machines whose task requires higher levels of 'algorithmic and hardware sophistication' and the ability to operate in the face of uncertainty .... [A] self-governing system is more likely to be described as 'autonomous' where human observers lack the ability to precisely foresee the exact sequence of steps that the system must take in order to complete its assigned task (or, equivalently, cannot foresee all events that will transpire when the system is activated).[6]

Others have noted, 'A system with a high level of autonomy is one that can be neglected for a long period of time without [human] interaction'.[7]

There is a modest level of autonomy in any system that achieves goals previously programmed by its operator without needing to receive instructions from the operator on an ongoing basis.[8] As the task or the environment in which the system is operating becomes more complex, autonomous systems will require more complex coding to achieve the operator's desired result.[9] This might be the case, for instance, when a State's military expects that its system will encounter a 'high degree of uncertainty in the environment in which it operates', perhaps because it may confront an adversary's autonomous system.[10] The more self-adaptive a cyber system is, the more likely it is that the system will be able to operate in those uncertain environments.[11] It is possible to design systems so that they do not need 'detailed foreknowledge of all combinations of circumstances which the software entity may encounter once it is in operation'; other systems may learn 'online' once deployed.[12] Such systems fall on the higher end of autonomy.

5 Tim McFarland, 'The Concept of Autonomy', this volume, ch 2, at 35 ('Autonomy is inherently a matter of degree'.); Defense Science Board, 'The Role of Autonomy in DoD Systems' (US Department of Defense 2012) 4 <https://fas.org/irp/agency/dod/dsb/autonomy.pdf> (noting that 'system autonomy is a continuum').
6 McFarland (n 5) 16–17.
7 Michael A Goodrich and Alan C Schultz, 'Human-Robot Interaction: A Survey' in Youn-kyung Lim (ed), *Foundations and Trends in Human-Computer Interaction* (Korea Advanced Institute of Science and Technology 2007) 203, 217.
8 McFarland (n 5) 21–22.
9 ibid 22.
10 ibid 23.
11 ibid 23–24 (discussing self-adaptive systems).
12 ibid 25.

B THE COMING OF INCREASED CYBER AUTONOMY

The trend toward increasing autonomy across weapons and weapons systems is pronounced. In his book Army of None, Paul Scharre predicts that this same trend will manifest itself in cyberweapons. He writes, 'Cyberweapons of the future — defensive and offensive — will incorporate greater autonomy, just the same way that more autonomy is being integrated into missiles, drones, and physical systems like Aegis'.[13] Indeed, another scholar notes that States already are widely deploying autonomous cyberweapons.[14] Stuxnet is an example of a cyber operation that entailed considerable autonomy: the cyber worm that the United States and Israel reportedly directed against Iran's nuclear centrifuges was 'an autonomous goal-oriented intelligent piece of software capable of spreading, communicating, targeting and self-updating'.[15]

There are at least two reasons why States increasingly will rely on autonomy in their cyber operations. First, and most obviously, the speed of adversaries' offensive cyber operations requires States to *defend* their systems at the same battle speed — which may be faster than a human can react. States will need to rely on some level of autonomy to have a chance at successfully defending their systems.[16] In the United States, a 2016 Defense Science Board (DSB) report described existing autonomous systems that 'carry out real-time cyber defense' while 'also extract[ing] useful information about the attacks and generat[ing] signatures that help predict and defeat future attacks across the entire network'.[17] It also cited a tool called Tutelage, which autonomously inspects and analyzes three million packets per second on an unclassified Defense Department computer system to prevent attacks.[18] The DSB report further imagined the existence of autonomous systems 'to control rapid-fire exchanges of cyber weapons and defenses', which would seem to require greater

13 Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (WW Norton 2018) 222.

14 Rebecca Crootof, 'Autonomous Weapons and the Limits of Analogy' (2018) 9 Harvard National Security Journal 51, 81; see also Rain Liivoja, Maarja Naagel and Ann Väljataga, 'Autonomous Cyber Capabilities Under International Law' (NATO CCDCOE 2019) 11–12 <https://ccdcoe.org/library/publications/autonomous-cyber-capabilities-under-international-law/> (discussing existing defensive and offensive cyber capabilities).

15 Stamatis Karnouskos, 'Stuxnet Worm Impact on Industrial Cyber-Physical System Security' (Paper presented at IECON 2011 — 37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, 7–10 November 2011) <https://ieeexplore.ieee.org/document/6120048>.

16 Crootof (n 14) 81 (noting that 'the speed of cyber will nearly always require that countermeasures be automated or autonomous to be effective').

17 Defense Science Board, 'Summer Study on Autonomy' (US Department of Defense 2016) 92 <https://www.hsdl.org/?view&did=794641>.

18 ibid 58.

elements of autonomy than packet inspection systems.[19] The US government seems to have pursued those systems. In 2017, the Defense Innovation Unit Experimental contracted for the Voltron project, which uses artificial intelligence to 'automatically detect, patch and exploit existing software vulnerabilities'.[20] The contract outlined defense use cases, but the system also 'has the potential to be used for offensive hacking purposes'.[21]

Second, deploying *offensive* cyber systems that are increasingly autonomous will make it easier for States to identify and then exploit adversaries' cyber vulnerabilities[22] because the systems can take advantage of machine-learning tools. These tools can identify patterns or abnormalities among vast quantities of data, which is helpful when trying to detect flaws in and infiltrate adversaries' cyber defenses. As James Johnson and Eleanor Krabill note, 'The machine speed of AI-augmented cyber tools could enable even a low-skilled attacker to penetrate an adversary's cyber defenses. It could also use advanced persistent threat tools to find new vulnerabilities'.[23]

Of course, defensive and offensive uses of autonomous cyber systems are interconnected. Even if States would prefer to use autonomous cyber systems solely in a defensive posture, Eric Messinger argues that the development of cyber defenses means that 'the development and deployment of offensive [autonomous cyber weapons] may well be unavoidable'.[24] Messinger notes,

> Powerful trends will exist toward optimizing offensive operations in cyber, and the paths of development for offensive malware could increasingly involve autonomous agents. Consider, for instance, a Washington Post report on the NSA's proposed use of a system, 'code-named TURBINE, that is capable of managing "potentially millions of implants"' — e.g., sophisticated malware — 'for intelligence gathering "and active attack"'. Though the details would matter for classifying such a system

19 ibid 4.
20 Chris Bing, 'The Tech Behind the DARPA Grand Challenge Winner Will Now Be Used by the Pentagon' (*Cyberscoop*, 11 August 2017) <https://www.cyberscoop.com/mayhem-darpa-cyber-grand-challenge-dod-voltron/>.
21 ibid.
22 United Nations Institute for Disarmament Research ('UNIDIR'), 'The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapons and Cyber Operations' (2017) 4 <https://unidir.org/files/publications/pdfs/autonomous-weapon-systems-and-cyber-operations-en-690.pdf>; Eric Messinger, 'Is It Possible to Ban Autonomous Weapons in Cyberwar?' (*Just Security*, 15 January 2015) <https://www.justsecurity.org/19119/ban-autonomous-weapons-cyberwar/>.
23 James Johnson and Eleanor Krabill, 'AI, Cyberspace, and Nuclear Weapons' (*War on the Rocks*, 31 January 2020) <https://warontherocks.com/2020/01/ai-cyberspace-and-nuclear-weapons/>.
24 Messinger (n 22).

> as autonomous, as opposed to 'semi-autonomous' or automated, it is easy to envision capabilities in the medium-term for which no other description is possible.[25]

Scharre contemplates a world in which offensive cyber operations go a step further. Instead of simply developing tools that actively manage implants or seek out enemy vulnerabilities, Scharre speculates that States might develop cyber tools that, once deployed, can fix themselves in the field and resist attack. He notes, 'Adaptive malware that could rewrite itself to hide and avoid scrutiny at superhuman speeds could be incredibly virulent'.[26] In the Defense Advanced Research Projects Agency's 2016 Grand Cyber Challenge, ForAllSecure's system was 'capable of automatically healing a friendly system while simultaneously scanning and attacking vulnerabilities in adversary systems'.[27] The US National Security Agency reportedly developed, or at least sought to develop, a system that would employ algorithms that constantly analyze metadata to detect malicious patterns, stop those attacks and autonomously initiate retaliatory counterattacks.[28] Others have envisioned decentralized swarms of autonomous agents that could attack systems without the need for centralized command and control.[29]

The United States is not the only State interested in bolstering the autonomy of its cyber operations. The United Kingdom has expressed an interest in pursuing autonomous cyber weapons as well.[30] Russian officials have stated that they view artificial intelligence as 'a key to dominating cyberspace and information operations', which suggests they intend to rely on certain levels of autonomy to achieve that goal.[31] China, too, appears committed to developing autonomous cyber capabilities.[32]

25 ibid.
26 Scharre (n 13) 226; see also Alessandro Guarino, 'Autonomous Intelligent Agents in Cyber Offense' in Karlis Podins and others (eds), *2013 5th International Conference on Cyber Conflict* (NATO CCDCOE 2013) (envisioning autonomous agents that are able to identify 'possible threats from defenders' and 'prevent and react to countermeasures').
27 Bing (n 20).
28 Nicholas Sambaluk (ed), *Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, and Technology* (ABC-CLIO 2019) 55.
29 Guarino (n 26).
30 United Kingdom, *National Cyber Security Strategy 2016–2021* (2016) [7.3.6] <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>.
31 Peter Apps, 'Are China, Russia Winning the AI Arms Race?' (*Reuters*, 15 January 2019) <https://www.reuters.com/article/us-apps-ai-commentary/commentary-are-china-russia-winning-the-ai-arms-race-idUSKCN1P91NM>.
32 Bill Gertz, 'US and China Racing to Weaponize AI' (*Asia Times*, 7 November 2019) <https://asiatimes.com/2019/11/us-and-china-racing-to-weaponize-ai/> (stating that 'Chinese multi-domain AI warfare will expand the battlespace from traditional air, sea, and land, to … cyberspace' and discussing military operations to include 'electronic countermeasures' and 'cybertakeover').

Although fully autonomous offensive cyber systems may remain speculative today, they lie within the realm of possibility. It is therefore worth considering how these tools — or even systems with moderate levels of autonomy — might escalate low-level cyber exchanges into uses of force that implicate international and domestic laws, or at least leave States poised on the brink of armed conflict.

C HOW CYBER AUTONOMY COULD LEAD TO HOSTILITIES

Cyber operations have the capacity to cause physical damage and, potentially, human harm. To date, very few of the known cyber operations have caused levels of damage that constitute uses of force or armed attacks under the UN Charter.[33] Yet States clearly have contemplated that cyber operations could produce such a result. Former US State Department Legal Adviser Harold Koh noted, for instance, 'Commonly cited examples of cyber activity that would constitute a use of force include, for example: (1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes'.[34] These types of operations, though still unrealized, are well within the realm of the possible, whether States or non-state actors commit them using cyber attacks with low or high levels of autonomy.

Even if an initial offensive cyber operation does not rise to the level of a use of force, some scholars have argued that the cyber domain is one in which escalation is likely.[35] Because it is harder to predict the impact of a given cyber operation than to predict the impact of a missile, there is greater room for miscalculation, even if the victim State intends to respond in a proportionate manner. As Scharre notes, 'You can have an accident that spirals out of control very badly that has a widespread effect

33 Gary Corn and Eric Jensen, 'The Use of Force and Cyber Countermeasures' (2018) 32 Temple International & Comparative Law Journal 127 (noting that 'most unfriendly acts between nations fall below the use of force').

34 Harold Hongju Koh, 'International Law in Cyberspace' (US Department of State, Remarks at the USCYBERCOM Inter-Agency Legal Conference, 18 September 2012) <https://2009-2017.state.gov/s/l/releases/remarks/197924.htm>.

35 See, eg, Herbert Lin, 'Escalation Dynamics and Conflict Termination in Cyberspace' (2012) 6 Strategic Studies Quarterly 46; Michèle Flournoy, Avril Haines and Gabrielle Chefitz, 'Building Trust through Testing' (*WestExec*, October 2020) 8 <https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf> ('The potential for unintended engagement or escalation is even greater when US and/or adversary systems have the sorts of advanced autonomy features that deep learning can enable, and their interaction cannot be studied or fully tested in advance of deployment'.).

in ways that are not possible with people' because humans cannot make the same number of errors as fast.[36] It also can be hard for States to signal their intentions in cyberspace, and those signals are an important way to avoid inadvertent escalation.[37]

Other scholars have suggested that concerns about cyber escalation are overblown. One pair of scholars, for instance, notes the world has seen little such escalation to date, perhaps because the tools and knowledge about vulnerabilities that a State needs to retaliate in cyberspace may not exist at the time the responding State needs them.[38] Further, decision-makers may be hesitant to respond to hostile cyber operations in some circumstances.[39]

Some of these constraints on escalation may weaken, however, when a State employs highly autonomous cyber systems. First, highly autonomous systems might by their nature be able to penetrate adversary systems more quickly and deftly than human-in-the-loop systems, requiring fewer advanced manual efforts to develop targets. Second, assuming that clear signaling is a good way to avoid unintended escalation, it may be harder for State operators to signal their intent to adversaries in advance of or during an autonomous cyber operation when those specific operations may happen without human pre-planning and possibly without knowledge of the opponent's identity. Third, highly autonomous cyber tools may act less predictably than human-in-the-loop systems, especially when confronting other autonomous systems. A UN report noted,

> As with the occasional stock market 'flash crashes', different algorithms — and even systems with very little autonomy — may interact in unforeseen ways before a human has time to intervene. … Emergent effects (unplanned and unintended) arise from interaction between the systems, and these effects are by definition

36 Johanna Costigan, 'Four Specialists Describe Their Diverse Approaches to China's AI Development' (*New America*, 30 January 2020) <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/four-specialists-describe-their-diverse-approaches-chinas-ai-development/>.

37 Brandon Valeriano, 'Managing Escalation Under Layered Cyber Deterrence' (*Lawfare*, 1 April 2020) <https://www.lawfareblog.com/managing-escalation-under-layered-cyber-deterrence>.

38 See Erica Borghard and Shawn Lonergan, 'Cyber Operations as Imperfect Tools of Escalation' (2019) 13 Strategic Studies Quarterly 122; see also Sarah Kreps and Jacquelyn Schneider, 'Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics' (2019) 5 Journal of Cybersecurity 1; Valeriano (n 37) (arguing that the cyber domain is not 'escalation dominant' but noting that there is 'no uniform view of how escalation should work in cyberspace').

39 See Borghard and Lonergan (n 38); Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press 2013) (arguing that the real threats are espionage, sabotage, and subversion, not armed conflict initiated in cyberspace); Jon Randall Lindsay, 'Restrained by Design: The Political Economy of Cybersecurity' (2017) 19 Digital Policy, Regulation & Governance 493.

> unpredictable, so our ability to plan for how to mitigate their consequences is poor.[40]

Fourth, even if a State itself takes steps to avoid a 'flash conflict' between its own cyber algorithm and another actor's algorithm, a third State could deliberately design a cyber operation to trigger this type of event between two of its adversaries.[41] Particularly for autonomous systems driven by artificial intelligence, 'autonomy itself will likely increase a military's vulnerability to cyberattacks' because artificial intelligence can increase the anonymity of attacks in cyberspace and thus facilitate an adversary's efforts to 'use malware to take control, manipulate, or fool the behavior and pattern-recognition systems of autonomous systems'.[42] These factors, taken together, suggest that autonomous systems may be susceptible to escalating cyber hostilities, even if States do not engineer them to be so.

None of this is to suggest that the developers of highly autonomous systems lack control over the parameters of their systems; after all, the 'behaviour of an autonomous system ultimately depends upon actions of people in relevant positions, notably its designer and operator, due to the nature of computers and software'.[43] What it does suggest is that a highly autonomous system may not act entirely predictably on its own, especially if it relies on machine learning, and it may act especially unpredictably when it confronts another actor's autonomous system. It is this situation — when the system deviates in problematic ways from decisions that a human would have made had the human undertaken the task — that gives rise to new types of democratic and strategic concerns.

D AUTONOMY AND INTERNATIONAL LAW

Notwithstanding these looming problems with increased autonomy, international law does not expressly prohibit States from using autonomous cyber tools. Although many States have agreed that existing bodies of international law — including the UN Charter and the laws of armed conflict — apply in cyberspace, those laws do not specifically preclude the

40 UNIDIR (n 22) 9.
41 ibid 10.
42 Johnson and Krabill (n 23).
43 McFarland (n 5) 20; see also Defense Science Board (n 5) 1–2 ('[A]ll autonomous systems are supervised by human operators at some level, and autonomous systems' software embodies the designed limits on the actions and decisions delegated to the computer'.).

use of autonomous systems or weapons. Instead, States are governed by the traditional *jus ad bellum* rules that regulate their resort to force and jus in bello rules that regulate the conduct of armed conflict, whether they use autonomous cyber tools or not. This means that States have a legal obligation to ensure that they deploy autonomous cyber systems in a way that comports with those rules. It would be lawful, for instance, for a State to 'produce and rely on machine-learning algorithms that allow them to defend' against cyber armed attacks 'at the speed of light, in what may come to look like automatic self-defense',[44] as long as those algorithms act consistent with the customary international law rules of necessity and proportionality.[45] States that deploy autonomous cyber tools during armed conflict will need to ensure that those tools can comply with the *jus in bello* requirements of distinction, proportionality, and precautions. Finally, concepts of state responsibility may help deter States from engaging in internationally wrongful acts while using autonomous cyber tools.

That said, building autonomous cyber systems that are able to detect when an incoming operation rises to the level of an armed attack, determine whether a cyber use of force is necessary in response, and initiate a cyber self-defense operation that is proportional to the incoming attack is easier said than done, as both a legal and practical matter. Former US Deputy Secretary of Defense Robert Work was willing to accept the possibility that the United States might need to deploy automated cyber counterattacks but recognized that delegating authority to autonomous or automated systems comes with risks. He noted that a 'machine might launch a counter cyber attack' and inadvertently cause an airplane to crash, for example, something that might violate the rules of the *jus ad bellum* and *jus in bello*.[46] Further, because cyberattacks are likely to be 'disguised by being routed through third-party machines, such as an unwittingly infected botnet or third-party private or public servers', autonomous responses risk targeting entities other than the State that initiated the attack.[47] An unwitting third-party State that suddenly faces

44 Ashley Deeks, Noam Lubell and Daragh Murray, 'Machine Learning, Artificial Intelligence, and the Use of Force by States' (2019) 10 Journal of National Security Law & Policy 1, 7.

45 Although most states have accepted that the UN Charter and the right to self-defense attach in the cyber setting, a few States have resisted this idea, including Cuba. See Michael Schmitt and Liis Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms' (*Just Security*, 30 June 2017) <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/>.

46 See Liivoja, Naagel and Väljataga (n 14) 23 (discussing autonomous responses that could violate the *jus ad bellum* and *jus in bello*).

47 Thomas Remington and others, 'Toward US–Russian Bilateral Cooperation in the Sphere of Cybersecurity' (Working Group on Future of US–Russia Relations 2016) 14 <https://futureofusrussiarelations.files.wordpress.com/2016/06/wg_working_paper7_cybersecurity_final.pdf>. This is not to suggest that such mistakes could never happen in human-in-the-loop cyber responses.

hostile cyber operations from the original victim may well respond in kind, setting the stage for unintended conflict.

Autonomous activities in cyberspace thus risk escalating cyber interactions to levels that violate international law, and possibly even to levels that constitute armed attacks that would trigger the adversary's right to self-defense. Delegating the authority to an autonomous system to decide when to respond to incoming attacks and effectively go on the counter-offensive 'could be very dangerous'.[48] This is especially true when States have asserted that they will only decide that something constitutes an armed attack based on a range of factors, including the apparent intent of the attacker and its identity.[49] It would be virtually impossible for an autonomous cyber system today to ascertain and evaluate factors such as intent before taking a response in national self-defense.

This all assumes that States would launch offensive or counter-offensive autonomous systems into the ether without plans to maintain meaningful control over them. It is far from clear that States such as the United States would do so. For instance, to help avoid consequences such as unintentional airplane crashes as the result of autonomous cyber operations, then-Deputy Secretary Work envisioned a role for scientists, lawyers and ethicists; automated safeties; and human oversight of the autonomous systems.[50] Others have noted that 'command and control of a true autonomous agent, especially a purely computational one … would have to translate chiefly in precise specifications of the agent's target and objectives — the goals — or, in military terms, in precise briefings before any mission'.[51] In short, there are strategic measures that States should take to avoid unintended escalation and conflict when deploying highly autonomous cyber systems.[52] The fact remains, however, that unless carefully managed, autonomous cyber exchanges risk escalating offensive and counteroffensive operations to a point that could trigger one State's right of self-defense and bring two States into hostilities without considered governmental decisions to do so.

48 Scharre (n 13) 223.
49 See Koh (n 34) ('In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues.').
50 Scharre (n 13) 228.
51 Guarino (n 26).
52 See Part V.

III
LEGISLATIVE ROLES IN USES OF FORCE AND OTHER MILITARY OPERATIONS

Part II illustrated that a range of States are likely to pursue high levels of cyber autonomy in an effort to protect their military systems and that such autonomy, unless carefully managed, raises the prospect of deliberate or unplanned escalation into hostilities. In light of this, how can States ensure that their governments deploy cyber autonomy in a manner consistent with their constitutions and laws?[53] In particular, how should legislatures regulate autonomous cyber tools to ensure that their executive branches remain faithful to domestic and international law regulating the resort to interstate force or other military operations?[54] This Part considers the several roles that legislatures play today in authorizing or overseeing their executives' military operations, to set the stage for Part IV's analysis of how cyber autonomy may alter those dynamics.

A DEMOCRACIES AND MILITARY OPERATIONS

Several scholars have examined the extent to which legislatures play a role in States' decisions to use interstate force and therefore provide democratic accountability for those choices. In 1996, Lori Damrosch, for instance, identified a trend toward a greater legislative role in State decisions to resort to force.[55] In 2003, she asserted that 'democratic parliaments [] play active roles in determining the scope and terms of national commitments to multilateral peace operations' such as the

53 We should also care about the extent to which the use of autonomous cyber tools comports with *international* law — and in particular the *jus ad bellum* and *jus in bello*. See, eg, Liivoja, Naagel and Väljataga (n 14); Guarino (n 26) (discussing the applicability of those bodies of law to autonomous cyber agents).

54 Some scholars argue that remote warfare technologies are intended to subvert democratic control of war. See, eg, Peter Singer, 'Do Drones Undermine Democracy?' (*Brookings Institution*, 22 January 2012) <https://www.brookings.edu/opinions/do-drones-undermine-democracy/> (arguing that 'new technology is short-circuiting the decision-making process for what used to be the most important choice a democracy could make'). This article assumes, however, that democratic states such as those in NATO wish to retain democratic accountability for their use of autonomous military systems.

55 Lori Damrosch, 'Is There a General Trend in Constitutional Democracies Toward Parliamentary Control over War-and-Peace Decisions?' (1996) 90 Proceedings of the ASIL Annual Meeting 36.

operations in the First Gulf War and Kosovo.[56] Other scholars have argued that since 1990, legislatures, at least in Europe, have sought to expand their involvement in decisions to use force abroad.[57]

One reason why it matters whether legislatures play a role in a State's decisions to deploy forces abroad or resort to force outside its territory is that mature democracies usually do not go to war with each other; they also are more likely to win the wars that they fight against autocratic states.[58] This suggests that there are virtues to retaining a healthy role for democratic legislatures in war-making decisions because they may help their States avoid 'bad' wars and fight only 'good' wars.[59] Tom Ginsburg notes,

> The democratic advantage in war, some theorize, results from the need to mobilize support among the public before going to war. Legislatures can play a role here, most obviously … by requiring evidence to justify wars …. Another source of democratic advantage is signaling: when the debate about going to war takes place in public and results in a decision to fight, the counterparty can more reliably assume that the state in question is really committed. This might lead the counterparty to back down ….[60]

In other words, the legislative role in making decisions to use force may play an important role in determining whether and when States go to war and whether they win those wars.

B SPECIFIC LEGISLATIVE ROLES IN WAR-MAKING

Even if many State constitutions and laws assign legislatures some role in making decisions about initiating and conducting war, not all systems

56 Lori Damrosch, 'The Interface of National Constitutional Systems with International Law and Institutions on Using Military Forces: Changing Trends in Executive and Legislative Powers' in Charlotte Ku and H Jacobsen (eds), *Democratic Accountability and the Use of Force in International Law* (Cambridhe University Press 2003) 39, 58 (noting that '[o]nly when military policies are fully debated and understood through the constitutional processes of democratic societies will there be sufficient assurance of public support for them').

57 Anne Peters, 'The (Non-)Judicialisation of War: German Constitutional Court Judgment on Rescue Operation Pegasus in Libya of 23 September 2015 (Part 1)' (*EJIL Talk!*, 21 October 2015) <https://www.mpil.de/files/pdf4/Peters_EJILTalk-The_Non-Judicialisation_of_War_Pegasus1.pdf>.

58 Tom Ginsburg, 'Chaining the Dog of War: Comparative Data' (2014) 15 Chicago Journal of International Law 138, 139 (discussing the democratic peace literature).

59 This is particularly true for multi-party systems, where legislatures are more likely to serve as a veto point. Legislatures in single-party systems or parliamentary systems in which the executive comes from a strong majority party may play a weaker role in checking the executive's resort to force.

60 Ginsburg (n 58) 146.

work identically. Some constitutions envision a role for legislatures to approve the use of force or troop deployments *ex ante*, while others authorize legislatures to approve or condemn executive decisions *ex post*. Legislatures also may oversee the executive's military strategy, hold votes of 'no confidence' and approve conflict-related expenditures. This section briefly details these distinct roles to set the stage for understanding how cyber autonomy might affect these roles in the future.[61]

1 *Authorizing Force ex ante*

Some constitutional systems envision a role for legislatures in authorizing force *ex ante.* The Czech Republic, Denmark, Germany, Hungary, Italy, Norway, Netherlands, Sweden and Mexico all ostensibly require prior parliamentary approval before the executive may send troops abroad.[62] In Sweden, for instance, the government can only send armed forces abroad in accordance with a specific law that sets forth the grounds for such action.[63] The German Constitutional Court has held that German armed forces can only be deployed abroad for non-defensive purposes with prior legislative approval.[64] In contrast, the legislatures of Belgium, Canada, France, Spain, the United Kingdom and the United States lack the right of prior authorization in most cases.[65]

In the United States, for instance, the executive currently interprets the Constitution to allow it to use force abroad without advance congressional authorization except in a limited set of cases in which the number of troops and the circumstances in which they would be deployed rise to the level of 'war in a constitutional sense'.[66] In the United Kingdom, the British government possesses prerogative powers to deploy the UK armed forces, and therefore historically did not seek legislative permission in advance to do so. In 2011, however, the government acknowledged that a new expectation had emerged that the House

61 Hans Born and Heiner Hänggi, 'The Use of Force under International Auspices: Strengthening Parliamentary Accountability' (Geneva Centre of the Democratic Control of Armed Forces 2005) <https://www.dcaf.ch/sites/default/files/publications/documents/pp07_use-of-force.pdf>.

62 ibid 8 (including citations to relevant provisions). For Mexico, see *Constitución Política de los Estados Unidos Mexicanos* [Constitution] art 89, § VIII (giving the President the power to declare war, 'having the previous authorization of the Congress') art 73, § XII (giving Congress the power to declare war). Of course, the start of a cyber conflict would not entail sending troops abroad, but could quickly transition to that.

63 Born and Hänggi (n 61) 7; Government of Sweden, Sveriges Riksdag, *The Constitution of Sweden: The Fundamental Laws and the Riksdag Act* (2016) 50 <https://www.riksdagen.se/globalassets/07.-dokument--lagar/the-constitution-of-sweden-160628.pdf>.

64 Russ Miller, 'Germany's Basic Law and the Use of Force' (2010) 17 Indiana Journal of Global Legal Studies 197, 202.

65 Born and Hänggi (n 61) 6 and 7.

66 See, eg, Memorandum from Assistant Attorney General Steven A Engel to Counsel to the President, April 2018 Airstrikes Against Syrian Chemical-Weapons Facilities (31 May 2018) <https://www.justice.gov/olc/opinion/file/1067551/download>.

of Commons would have the chance to debate the deployment of military forces in advance, except in an emergency.[67] That new convention was put to the test when the UK government sought legislative approval in 2013 for military action in Syria and Parliament voted it down. However, the UK undertook limited airstrikes against Syrian chemical weapons capabilities in 2018 without consulting Parliament first, suggesting that the government will only follow the convention where possible military action is premeditated and will entail the deployment of military forces in an offensive capacity.[68]

One obvious benefit to legislative participation in decisions to resort to force in the first instance is that legislatures can constrain 'overzealous executives by requiring evidence to justify wars'.[69] As Ginsburg notes, the Framers of the US Constitution believed that congressional involvement in decisions related to force would slow down war-making except in true emergencies. For democracies today, such deliberation may help '"screen" wars: ensuring that the conflicts that the nation enters into are "good" wars, while eschewing "bad" wars'.[70]

A constitutional requirement of *ex ante* authorization is a powerful tool for legislatures compared to *ex post* powers because the introduction of troops often operates as a one-way ratchet. Once a State has committed troops to a conflict, legislatures have a hard time voting to withdraw those troops because doing so may be seen by the public as unpatriotic or a sign of weakness.[71] Therefore, legislatures that have a role in authorizing force *ex ante* have far more leverage in the decision-making process than do those whose only authorizing role arises after the fact.

Nevertheless, most systems that give their legislature *ex ante* powers include an exception that allows the executive to respond to imminent attacks or emergencies without advance legislative approval.[72] Even the

67 United Kingdom, House of Commons, *Parliamentary Approval for Military Action* (17 April 2018) <https://commonslibrary.parliament.uk/research-briefings/cbp-7166/>.

68 ibid. Most uses of highly autonomous cyber operations would not meet that test.

69 Ginsburg (n 58) 146.

70 ibid 142, 145; Yasuo Hasebe, 'War Powers' in Michel Rosenfeld and Andras Sajo (eds), *Oxford Handbook of Comparative Constitutional Law* (Oxford University Press 2012) 465 (noting that legislative approval for armed force provides more legitimacy and popular support for the operations).

71 See, eg, *Mitchell v Laird*, 488 F2d 611 (DC Cir 1973) (discussing why members of Congress who opposed the continuation of the Vietnam War might nevertheless vote to appropriate money, to avoid abandoning the forces already fighting).

72 See, eg, *Regeringsformen* [Constitution] 15:13 (Sweden) (giving the government the right to deploy Swedish armed forces to meet an armed attack on Sweden or prevent a violation of Sweden's territory); *The Prize Cases*, 67 US (2 Black) 635 (1863) (implying a presidential 'repel attacks' power); *Grondwet voor het Koninkrijk der Nederlanden* [Constitution] art 96, sub 2 (Netherlands) ('approval [for a declaration of a state of war] shall not be required in cases where consultation with Parliament proves to be impossible as a consequence of the actual existence of a state of war'), *Glasilo Uradni List Republike Slovenije* [Constitution] art 92 (Slovenia); *Eesti Vabariigi põhiseadus* [Constitution] arts 65, sub 15, 128 (Estonia); *Türkíye Cumhuríyetí Anayasasi* [Constitution] art 92 (Turkey).

laws of a State such as Germany, in which both the legislature and the judiciary play significant roles in decisions about the resort to force, contemplate that there will be situations of 'imminent danger' in which the executive must act on its own without pre-approval by the legislature.[73] In such cases, however, the executive must promptly seek approval from the German parliament afterwards.[74]

One way that legislatures can implement their *ex ante* authority is to enact laws that stipulate the settings in which and adversaries against whom the executive is authorized to use force. In the United States, these often take the form of Authorizations to Use Military Force (AUMFs). In a little-noticed statute in 2018, Congress accorded the President authority akin to an AUMF for certain cyber operations. Section 1642 of the John McCain National Defense Authorization Act (NDAA) for FY 2019 states,

> In the event that the National Command Authority [i.e., the President and the Secretary of Defense] determines that the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, or Islamic Republic of Iran is conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, … the National Command Authority may authorize the Secretary of Defense, acting through the Commander of the United States Cyber Command, to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter such attacks ….[75]

When the Defense Department employs this authority, the Secretary of Defense must report to the congressional defense committees no later than forty-eight hours after the operation; must include the actions in a quarterly report to the defense committees; and must report annually to the congressional defense, intelligence and foreign affairs committees about the 'scope and intensity' of the cyber attacks on the United States.[76] Although the provision does not resemble most of Congress's *ex ante* force

73 Peters (n 57).

74 *Parlamentsbeteiligungsgesetz* [Parliamentary Participation Act] § 5 (Germany); see also Hasebe (n 70) 478 (noting that the Japanese Self-Defense Forces Act provides that the Diet (national legislature) must authorize force in advance, except when there is no time to obtain such authorization, and that the Prime Minister 'may order the engagement of the [Self-Defence Forces] when an attack is clearly imminent and the necessity of the engagement is recognized').

75 John S McCain National Defense Authorization Act for Fiscal Year 2019, Pub L No 115-232, § 1642(a)(2), 1642(c), 132 Stat 1636 (2018) ('2019 NDAA').

76 ibid.

authorizations, 'it is an AUMF of a very narrow and specific variety'.[77] Part IV considers the effect of cyber autonomy on authorizations like this one.

2 *Ratifying Force ex post*

Another role for legislatures is to ratify or shape the executive's use of force *ex post*. Ginsburg, who reviewed 745 constitutions that entered into force since 1789, noted that since the early 1800s, constitutions have tended to assign the executive the power to resort to force. However, 'legislatures retain a major role in war policy' because they retain the power after the fact to approve or strike down the executive's decision to resort to force or to deploy troops.[78] France's current constitution, for instance, anticipates that its National Assembly must authorize declarations of war but 'includes no requirement that parliamentary authorization be prior to the declaration of war'.[79] For uses of force short of war, which include many forcible acts, the French executive must notify the Assembly of its decision to forcibly intervene abroad no later than three days after the intervention. The Assembly can debate the question, but does not actually vote on it, though if the intervention exceeds four months, the executive must ask the Assembly to authorize that extension.[80] Some States envision greater legislative control *ex post*. The laws of Denmark, Germany and the Netherlands, for example, contemplate not only that those legislatures will have powers of prior authorization but also that they will have the opportunity to subsequently approve the mission's mandate, operational guidelines and duration.[81]

Under a model of *ex post* legislative approval, it is possible that the executive will reject or ignore subsequent legislative condemnation of its troop deployments or other military operations. As noted above, though, the more likely scenario is that legislatures will find it hard not to support executive decisions, at least where the executive is responding to an actual attack on the country or where it has committed troops already. There is more political room for a legislature to condemn after the fact the executive's decision to use force or deploy troops where the forcible episode is completed quickly or there are few troops on the ground overseas.

77 Robert Chesney, 'The Law of Military Cyber Operations and the New NDAA' (*Lawfare*, 26 July 2018) <https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa> (noting that the US Congress has enacted at least two other provisions that bolster the Defense Department's ability to undertake cyber operations when appropriately authorized to do so); see 2019 NDAA (n 75) § 1632; 10 USC § 394 (2019); National Defense Authorization Act for Fiscal Year 2012, Pub L 112–81, § 954 (2011), 125 Stat 1551.

78 Ginsburg (n 58) 149–50.

79 Hasebe (n 70) 473 (discussing Article 35 of the French Constitution).

80 Hasebe (n 70) 474–5.

81 Born and Hänggi (n 61) 8.

3 *Funding and oversight*

In addition to helping to regulate the initiation, conduct and cessation of military operations, legislatures play at least two other significant force-related roles. First, legislatures fund the military operations. This power of the purse can provide significant leverage over how and where the executive conducts those operations and the length of time for which the executive can fight. Like *ex post* ratifications, however, legislators may feel pressure to continue to fund conflicts they do not support because withholding funds from the troops risks seeming unpatriotic.[82]

Second, legislatures can conduct oversight for the duration of the conflict, to examine how the executive is conducting the conflict, whether it is exceeding its mandate, whether it is using resources wisely and whether the armed forces are complying with international and domestic laws.[83] Depending on the capacity of the legislative committees tasked with oversight responsibilities, these legislators can play an important role in holding the executive accountable for illegal, incompetent or unwise military and policy decisions.[84]

Even though most States authorize their executives to act without legislative approval in the face of imminent attacks, legislatures have a range of roles to play in authorizing their executives to use force, demanding justifications from the executives about the decision to enter into a conflict and generally enhancing democratic accountability for warfighting. A legislature's ability to enhance its executive's compliance with public law values — including international law — depends on a reliable flow of information between the executive and the legislature; on the legislature's competence to understand the strategy, tactics and tools that the executive is using; and on adequate time to make informed decisions. The introduction of significant levels of cyber autonomy into the mix is likely to complicate these already-challenging tasks.

82 See *Mitchell v Laird*, 488 F2d 611 (DC Cir 1973).

83 One salient example here is the US Congress's decision to try to terminate President Reagan's funding of the Contras in Nicaragua. See Boland Amendment, Pub L No 98-473, § 8066(a), 98 Stat 1837 (1984).

84 Ashley Deeks, 'Secrecy Surrogates' (2020) 106 Virginia Law Review 1395 (discussing these qualities as public law values).

IV
THE EFFECT OF CYBER AUTONOMY ON DEMOCRATIC ACCOUNTABILITY

Burgeoning cyber autonomy may affect democratic accountability for the use of force — as well as domestic checks and balances — in at least three ways. First, it may alter the balance of power between legislatures and executives, further empowering executives at the expense of legislative input about the timing, scope and legality of particular uses of force or offensive cyber operations. Second, it may alter the balance among a state's executive agencies. Third, it may alter power dynamics among different types of officials within those agencies. If obtaining the input of a diversity of executive officials and securing a legislative role in decisions about the use of force helps improve the quality of decision-making, the overall effect of robust uses of cyber autonomy may be to increase the potential for 'bad' conflicts between States.[85]

A ALTERING THE BALANCE BETWEEN LEGISLATURES AND EXECUTIVES

There are several ways in which autonomous cyber capabilities might further empower executives at the expense of the legislative role in force decisions, an imbalance that seems to dominate most governmental regimes today.[86] First, legislatures may suffer from information deficits about the existence and capabilities of the cyber systems. Second, there may be fewer opportunities temporally for legislators to weigh in about the wisdom of forcible responses. Third, executive reliance on highly autonomous systems may make it very hard for legislators to provide meaningful oversight *ex post*.

85 See Ginsburg (n 58) 145.

86 I do not mean to suggest that the growing autonomy of cyber operations is the only aspect of these operations that poses a threat to legislative capacity and oversight. For instance, the increased precision of cyber tools means that they can produce a more potent effect on the intended victim, which could increase the risks of escalation. Further, the growth of the Internet of Things and the interconnectedness of many publicly- and privately-owned systems means that there are more ways for a State's cyber operations to go wrong and have cascading, unintended effects. As with the growing autonomy of cyber systems, both of these developments make it critical for Congress to retain a role in oversight.

1 *Information Deficits*

Assume that a State's military develops autonomous cyber systems that can operate offensively or counter-offensively. An initial concern might be that legislators are unaware that the autonomous systems exist. Although legislatures sometimes appropriate money for specific programs, appropriations laws may not necessarily articulate in detail the types and nature of weapons that militaries are and are not authorized to develop. Legislators may also have difficulty obtaining information about executive cyber doctrines that will guide how the executives will utilize their cyber tools — including autonomous tools. In the United States, even though Congress has well-staffed committees that oversee the defense and intelligence agencies, and recently has legislated with particularity in the cyber area, Congress had difficulty gaining access to a classified US executive policy that sets out the approval process for conducting offensive cyber operations.[87] It stands to reason that Congress — let alone the legislatures of other States — might also have problems obtaining information about the extent of the human role in those cyber operations.

As a related matter, even if militaries share information with legislators about their cyber capabilities or doctrines, legislators may have difficulty understanding particular cyber capabilities, including autonomous capabilities and the risks attendant thereto. There are many reasons to think that the average legislator is not particularly savvy about technology.[88] In one salient example, several US senators proposed legislation in 2016 that would have required companies to provide the government with access to encrypted data when a court had so ordered. Critics savaged

87 Mark Pomerleau, 'After Tug-of-War, White House Shows Cyber Memo to Congress' (*Fifth Domain*, 13 March 2020) <https://www.fifthdomain.com/congress/2020/03/13/after-tug-of-war-white-house-shows-cyber-memo-to-congress/> (describing a multi-month struggle to obtain access to National Security Presidential Memorandum 13).

88 See Ashley Deeks, 'Facebook Unbound?' (2019) 105 Virginia Law Review Online 1, 6–7 (noting that members of Congress lack sophisticated understandings of how new technologies work); Matthew Scherer, 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies' (2016) 29 Harvard Journal of Law & Technology 353, 380 (noting that 'only the small subset of the legislature that sits of the relevant committee will hear the experts' testimony, and even those legislators cannot afford to spend an inordinate amount of time conducting hearings on any on particular issue'); Karen Hao, 'Congress Wants to Protect You from Biased Algorithms, Deep Fakes, and Other Bad AI' (*MIT Technology Review*, 15 April 2019) <https://www.technologyreview.com/2019/04/15/1136/congress-wants-to-protect-you-from-biased-algorithms-deepfakes-and-other-bad-ai/> (noting that 'only a handful of members of Congress have a deep enough technical grasp of data and machine learning to approach regulation in an appropriately nuanced manner'); Julia Black and Andrew Murray, 'Regulating AI and Machine Learning: Setting the Regulatory Agenda' (2019) 10 European Journal of Law and Technology 3, s 5 <https://ejlt.org/index.php/ejlt/article/view/722> ('[T]here is little evidence that regulators have the necessary capacity properly to evaluate all the actual and potential uses of AI in their regulatory domains. Asymmetries of knowledge and skills are amplified in the highly technical area of AI'.).

the bill, not only because they objected to the policy but also because the bill seemed to reflect a flawed understanding of encryption technology.[89]

To counter this deficit, the US Government Accountability Office — an agency within the legislative branch — has proposed setting up a new office to help Congress understand the impacts of technology-related policies that it pursues,[90] and others have suggested reviving the now-defunct Office of Technology Assessment, which provided Congress with scientific expertise to match that of the Executive Branch.[91] In the UK, a joint parliamentary committee has recommended that the Government Office for Artificial Intelligence and the Centre for Data Ethics and Innovation — which will consist of technical and ethics experts — should identify for Parliament any gaps in existing regulations, suggesting that Parliament itself must rely on outside experts for artificial intelligence-related analysis.[92] Legislatures with small defense committees may face particular challenges in overseeing cyber operations generally — to say nothing of highly autonomous cyber operations — because their legislators presumably are spread more thinly across issue areas. Further, if they have small budgets, they will be able to employ fewer staffers and can convene fewer hearings in which outside experts could help them understand the issues and technologies they confront.[93]

Even legislators with a basic understanding of cyber operations may not have a full appreciation for the risks of autonomous operations and may not be positioned to ask the right questions of the executive branch.

89 Julian Sanchez, 'Feinstein-Burr: The Bill that Bans Your Browser' (*Just Security*, 29 April 2016) <https://www.justsecurity.org/30740/feinstein-burr-bill-bans-browser/>.

90 Jack Corrigan, 'Inside GAO's Plan to Make Congress More Tech-Savvy' (*NextGov*, 20 March 2019) <https://www.nextgov.com/cio-briefing/2019/03/inside-gaos-plan-make-congress-more-tech-savvy/155689>; Cat Zakrzewski, 'These Scientists Are Trying to Help Congress Get Smarter About Tech' (*Washington Post*, 27 January 2020) <https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2020/01/27/the-technology-202-these-scientists-are-trying-to-help-congress-get-smarter-about-tech/5e2b1fcc602ff14e6605928f/>.

91 US Government Accountability Office, 'Office of Technology Assessment' (13 October 1977), <https://www.gao.gov/products/103962>. See also US House of Representatives, Congressional Artificial Intelligence Caucus <https://artificialintelligencecaucus-olson.house.gov> accessed 14 October 2020 (describing the 'AI Caucus' in Congress, created to 'inform policymakers of the technological, economic and social impacts of advances in AI' by bringing together academics, private sector officials, and government officials); Mike Miesen and others, 'Building a 21st Century Congress: Improving Congress's Science and Technology Expertise' (Belfer Center for Science and International Affairs, September 2019) <https://www.belfercenter.org/publication/building-21st-century-congress-improving-congresss-science-and-technology-expertise> (discussing Congress's demand for science and technology expertise and the root causes of its lack of technological capacity); Caroline Kenny and others, 'Legislative Science Advice in Europe: The Case for International Comparative Research' (2017) 3 Palgrave Communications 17030 (discussing the role for scientific advice in legislatures in the UK and Europe).

92 United Kingdom, House of Lords, Select Committee on Artificial Intelligence, 'AI in the UK: Ready, Willing and Able?' (2018) [386] <https://ec.europa.eu/jrc/communities/sites/jrccties/files/ai_in_the_uk.pdf>; see also United Kingdom, Office for Artificial Intelligence, <https://www.gov.uk/government/organisations/office-for-artificial-intelligence>.

93 For example, Hungary's Defense Committee had a budget of €4,000 ($4,800) in 2004: Born and Hänggi (n 61) 10.

Indeed, not all of the executive branch officials involved in decision-making may understand the capabilities and risks of complex, highly autonomous cyber systems. In the context of electronic surveillance systems, for example, in 2013 the US Director of National Intelligence (DNI) declassified a set of documents that revealed a lack of compliance with judicial mandates. The DNI explained that the compliance problems

> stemmed in large part from the complexity of the technology employed in connection with the bulk telephony metadata collection program, interaction of that technology with other NSA systems, and a lack of a shared understanding among various NSA components about how certain aspects of the complex architecture supporting the program functioned. These gaps in understanding led, in turn, to unintentional misrepresentations in the way the collection was described to the FISC.[94]

If some intelligence officials within a single agency were unclear about how the technology supporting an electronic surveillance program worked, it is easy to imagine how legislators would have had trouble understanding that program and — likewise — how they might struggle to understand very technical cyber tools that include significant levels of autonomy.

To some extent, this lack of understanding reflects a broader societal challenge posed by systems that rely on machine-learning tools. Those systems are often described as 'black boxes' because the weight that they give to factors within the data to reach predictions or recommendations is generally opaque. As a result, not only legislators but humans generally find it difficult to interpret or explain the outputs of systems that operate with high levels of autonomy. Computer scientists and militaries are keenly aware of this problem and are working to produce 'explainable' or 'interpretable' artificial intelligence, sometimes referred to as 'white box' models. As discussed below, legislatures have an opportunity to shape the level of explainability of the executives' cyber algorithms. Requiring executives to produce algorithms that are more transparent might also make it easier for legislators to hold executive actors accountable because

94 Office of the Director of National Intelligence, 'DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA)' (Press Release, 10 September 2013) <https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/927-dni-clapper-declassifies-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act-fisa>.

transparent algorithms might be easier to audit after the fact than human decisions are.

2 *Limited Opportunity for Legal and Policy Input*

In some States, legislatures can constrain 'overzealous executives by requiring evidence to justify wars'.[95] This is primarily true when the State's system contemplates legislative approval for the use of force *ex ante*. It also assumes that there is time for legislative input before the executive makes a decision to resort to force. But the US executive branch, for one, has taken the view that very few uses of force require congressional pre-authorization. If the only time *ex ante* congressional authorization for military operations is legally necessary is when the United States plans to deploy hundreds of thousands of troops abroad, cyber operations — whether human-in-the-loop or out-of-the-loop — will almost never reach the threshold of 'war in a constitutional sense'.[96] Hostile cyber exchanges, at least when the salvos remain within the cyber realm, are unlikely to pose an immediate and significant threat to US troops and will not trigger the need for congressional authorization under the 'Declare War' clause. Yet autonomous cyber systems may pose a reasonable chance of escalation — whether intended or unintended — such that legislative input might be normatively desirable *ex ante*. Even for States whose legal systems contain a clear *ex ante* requirement for legislative authorization, that authorization may be limited to troop deployments, which will not cover cyber exchanges, or may contain an emergency carveout, which would cover responses to sudden cyber attacks.[97]

As noted above, the US Congress has already provided limited *ex ante* authorization for the executive to 'take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter such attacks' when those systematic attack campaigns come from Iran, North Korea, Russia or China.[98] This provision may actually serve as a limitation on

95 Ginsburg (n 58) 146.

96 Matthew Waxman, 'Cyber-Attacks and the Constitution' (Aegis Series Paper No 2007, Hoover Institution 2020) 4–5 <https://www.hoover.org/sites/default/files/research/docs/waxman_webready.pdf > ('If war powers are a special constitutional category demanding formal congressional approval because of the risks to American blood, most cyber-attacks barely if at all implicate this concern, because the risks are so tiny and remote.'); Eric Jensen, 'Future War and the War Powers Resolution' (2015) 29 Emory International Law Review 499, 541 (noting that the War Powers Resolution's reporting threshold fails to encompass cyber operations).

97 That said, in the US, the President often complies with statutory restrictions on his use of the military, even as he asserts constitutional objections to those statutes. See David Barron and Martin Lederman, 'The Commander in Chief at the Lowest Ebb: A Constitutional History' (2008) 121 Harvard Law Review 941. Thus, it would be worthwhile for Congress — and possibly other legislatures — to carefully consider how to set boundaries on the use of autonomous cyber tools.

98 See 2019 NDAA (n 75) § 1642.

the use of autonomous cyber systems, as it requires the executive to identify the source of the hostile cyber campaign. Unless the executive's autonomous cyber system is crafted to respond only to hostile operations that bear attack signatures from the named States, the executive would have difficulty relying on this authorization to support the use of such a system.[99] As discussed in Part V, legislatures should consider providing this kind of advance authorization, which can both serve as permission for and constraint on the use of cyber autonomy.

3 *Time Constraints*

As a related matter, highly autonomous cyber systems narrow significantly whatever consultative role legislatures may retain for themselves, at least in the window before a specific forcible cyber exchange takes place. The most significant reason to deploy autonomous cyber tools is to allow the system to operate at lightning speeds. Yet it is already the case today — before the widespread use of highly autonomous cyber tools — that executives, acting in response to perceived imminent threats of armed attacks on their States, employ force without legislative approval or even consultation. These threats may mostly come from terrorists today, but it is increasingly possible to conceive of cyber attacks as creating situations in which executive officials will need to respond in a very short time frame.

Purely defensive autonomous cyber operations — those that use autonomy only to identify and fend off hostile cyber operations within one's own system — are unlikely to implicate congressional prerogatives, as these settings will fall within the executives' 'repel attacks' powers found in many States' constitutions. But 'offensive' cyber capabilities that leave one's own system,[100] even in an act of self-defense, are more likely to implicate those prerogatives because they increase the chance of escalation and error. Further, autonomous systems 'may operate at speeds that make it impossible for the operator to meaningfully intervene'.[101] Thus, once a State deploys an autonomous cyber tool that has the capacity to reach outside that State's own system and inflict substantial harm, there will be no opportunity for congressional consultation on particular operations.

99 However, the US executive might conclude that it could rely on its broad Article II powers, including the commander-in-chief power, under the Constitution, even if it lacked specific statutory authority to act. It is also possible that providing legislative authorization for the executive to use autonomous responses to cyber operations only when they come from certain States will stimulate other States to engage in false-flag attacks from one of the named States in an effort to escalate cyber hostilities between the victim State and the named State.

100 See Liivoja, Naagel and Väljataga (n 14) 12–13.

101 ibid 15.

4 *Challenges to ex post Oversight*

One of the more reliable roles for legislatures during a conflict is the provision of oversight. A legislative body can help unearth how conflicts started, whether the State is achieving its military and strategic goals and whether it is complying with domestic and international laws during the fight. Legislatures often rely on executive actors to provide information about the conflict, but legislators can also convene hearings of outside experts and collect open-source intelligence about the situation from journalists on the ground.

Cyber hostilities, particularly those conducted by highly autonomous systems, will be far harder to understand and oversee. Conducting forensic audits that recreate what happened during a cyber exchange and translate them into language that congressional overseers can understand will be more challenging than reviewing radar patterns or identifying the source of limpet mines found on oil tankers.[102] The use of artificial intelligence to facilitate autonomy will pose 'black box' problems for legislators who seek to audit how the cyber operations played out. Further, there will be no 'war zone' to which journalists or outside analysts can travel to talk to troops on the ground about what they are seeing. As a result, there will be far fewer open-source reports about what has transpired during these 'invisible' cyber operations, unless and until they morph into kinetic conflicts.

In the United States, Congress has begun to address this potential lack of visibility by mandating that the executive report to it after conducting certain types of cyber operations. As Matthew Waxman notes,

> Congress has mandated special reporting requirements for offensive and 'sensitive' cyber-operations to the armed services committees.[103] Cyber-attacks conducted as covert action by the CIA would be reported separately to the intelligence committees, as would other intelligence activities that might fit within the definition here of cyber-attacks. Such reporting is foundational to other congressional roles, because it keeps Congress — or at least

102 'Iran News: US Says Mines Used in Tanker Attacks Bear "Striking Resemblance" to Weapons Touted by Tehran' (*CBS News*, 19 June 2019) <https://www.cbsnews.com/news/iran-news-us-shows-limpet-mine-parts-case-against-iran-in-tanker-attacks-today-2019-06-19/>.

103 The 2013 NDAA required the Department of Defense to 'provide to the Committees on Armed Services of the House of Representatives and the Senate quarterly briefings on all offensive and significant defensive military operations in cyberspace carried out by the Department of Defense during the immediately preceding quarter'. National Defense Authorization Act for Fiscal Year 2013, Pub L No 112-239, § 939, 126 Stat 1632 (2012); 10 USC § 484 (2011). Congress updated and expanded this provision in the 2017 and 2019 NDAAs.

> certain committees — informed of executive branch actions that would otherwise be largely invisible.[104]

Existing statutes require the US military to report to the congressional defense committees within forty-eight hours when it conducts a cyber operation determined to have a medium or high probability of political retaliation, detection or collateral effects and is intended to cause effects in an area in which the United States is not already involved in hostilities.[105] This kind of requirement is helpful — at least on its face — because it puts some members of Congress on notice of situations that might lead to conflict. But a situation between two States could escalate significantly within forty-eight hours, particularly if the States involved are using autonomous systems that are not adequately engineered to avoid escalation and to minimize risks of misdirecting responses. Further, it is not yet clear how these reporting rules are functioning and whether Congress is receiving the information that it believes it needs to provide adequate oversight.[106]

B ALTERING THE BALANCE AMONG EXECUTIVE AGENCIES

The growth of autonomous cyber systems is likely to further alter the current balance between executives and legislatures in use of force decisions. But the use of autonomous cyber tools also has the potential to affect the balance of power within executive branches themselves. One interesting question is whether the use of high levels of cyber autonomy will continue to push power out to the militaries as the creators and operators of these autonomous tools, or whether it offers an unexpected opportunity to readjust and centralize the locus of some of the decision-making associated with these tools.

On its face, it might appear that highly autonomous cyber tools will empower militaries at the expense of other executive agencies that have important equities in foreign policy decision-making, such as foreign and justice ministries. Even if these other agencies are involved in discussions about cyber strategy, they likely lack the technological sophistication that

104 Waxman (n 96).
105 10 USC § 395 (2019).
106 Robert Chesney, 'The Domestic Legal Framework for US Military Cyber Operations' (Aegis Series Paper No 2003, Hoover Institution 2020) 15 <https://www.hoover.org/sites/default/files/chesney_webreadypdf.pdf>.

military coders and cyber operators possess and so may have difficulty understanding whether highly autonomous cyber tools advance or hinder certain policy objectives and what level of risk these systems pose. Further, as with any military operation, those who sit closest to the point of execution have the greatest power to make last-minute decisions and adjustments. Although autonomous systems will take some of that control from those cyber operators, those operators nevertheless have more direct 'eyes on' the operations and their effects. In the United States, Congress's recent legislative acts seem to have enabled this. As Waxman notes, 'Congress has clarified the Defense Department's authority to conduct offensive cyber-operations, thereby strengthening its position within the executive branch and facilitating action by alleviating legal doubts about its mandate'.[107]

However, there is a possibility that increased autonomy could reverse this flow of power to militaries. Increased autonomy in warfighting tasks may — perhaps ironically — offer the opportunity to centralize decision-making, as the process of building machine-learning algorithms for warfighting systems, including cyber systems, seeks to incorporate the commander's intent and remain sensitive to legal constraints. These centripetal forces may even mean that other national security agencies begin to play a role in developing the policies undergirding those algorithms.[108] In the United States, the National Security Council and the State Department, for instance, may seek to inform the algorithms' contents and structure to ensure that they comply with the laws of armed conflict and the UN Charter.

Today, the US military has a well-established weapons review process; non-military lawyers are not involved. Likewise, judge advocates provide legal advice to commanders during armed conflict without consulting the Defense Department's Office of the General Counsel, let alone the National Security Council or other executive agencies. And yet there may be pressure to adjust the traditional process when the government builds machine-learning systems that can undertake autonomous action during conflict. If the use of the system will have significant foreign relations implications and if the system's recommendations implicate legal questions that already have been the subject of significant interagency

107 ibid 10–11 (referring to 2012 NDAA, Pub L No 112-81, § 954 (2011)); 10 USC § 111 (2011); National Defense Authorization Act for Fiscal Year 2018, Pub L No 115-91, §1633(a), §1633(b)(5)(B), 131 Stat 1283 (2017).

108 Some of the discussion in this section is drawn from Ashley Deeks, 'Will Autonomy in US Military Operations Centralize Legal Decision-Making?' (*Articles of War*, 5 August 2020) <https://lieber.westpoint.edu/autonomy_military_operations_decision-making/>.

interest, other agencies' policymakers and lawyers may demand a role. The lawyers might want to craft guidance in advance about what types of autonomous cyber tools would or would not meet underlying international law standards, for instance. And because the coding process will involve decisions about the nuances of that law and will happen before the system is deployed, there may be greater opportunities for a broader set of US government actors to claim a stake in those decisions than there is in kinetic lethal operations downrange.

There would be both benefits and costs to such a development. Militaries likely would perceive this potential centralization of decision-making as unattractive and might resist sharing the authority to make algorithmic choices about autonomous cyber tools. Interagency lawyers might also struggle to reach consensus about what features to incorporate into those tools. On the other hand, obtaining interagency understanding and acceptance of autonomous cyber tools would bolster the military's confidence about their use and would also allow that State's diplomats and foreign ministry lawyers to engage more deeply with allies on what may be controversial uses of machine learning and cyber tools.

Whether the growth in cyber autonomy ends up diminishing or increasing the role of non-military executive agencies will depend on decisions made by legislatures, choices by executive branch leadership, and the efforts (or lack thereof) of civilian national security agencies to help define the parameters of autonomous cyber tools as they are developed.

C ALTERING THE BALANCE WITHIN EXECUTIVE AGENCIES

Finally, within individual executive agencies, autonomous cyber tools, like other high-technology tools, will almost inevitably empower operators and computer scientists over lawyers. As I have noted elsewhere, in contexts driven by high-technology problems, data scientists will become relatively more important to policymakers than they have been in the past, and senior officials may start to treat their input as just as important to an international law or foreign policy decision as that of their international lawyers. [109] In my view, 'It will be the data scientists who can suggest new text-as-data tools and interpret the results of existing models. This means that the data scientists who embrace and understand the problems

109 Ashley Deeks, 'High-Tech International Law' (2020) 88 George Washington Law Review 574, 647.

that international lawyers and diplomats face will be most effective in this setting'.[110] Among officials who are not cyber experts, military and civilian actors who are technologically literate will be empowered relative to those who disdain technology or are unable to grasp its basic capabilities, limitations, and risks.[111] Thus, lawyers and policymakers who seek to work with data scientists and programmers to understand autonomous cyber tools will gain power relative to their counterparts who cannot or will not do so.[112]

V
PRESERVING ACCOUNTABILITY

In light of the range of challenges to democratic accountability and oversight that high levels of cyber autonomy will pose, this Part considers steps that States might take to meet some of those challenges. A State's legislature, its executive branch and its allies all can take actions to ensure that the State's use of autonomous cyber tools remains responsive to democratic systems of governance.

A PRESERVING LEGISLATIVE PARTICIPATION

Legislatures could take at least two steps to help preserve a role for themselves in a world of autonomous cyber tools. First, they could bolster their own technological expertise and access to high-tech experts. Second, they could embrace the possibilities for legislation that sets appropriate parameters on the executive branch's development and use of highly autonomous cyber systems.

1 *Developing Expertise*

A range of scholars have suggested ways in which legislatures could improve their understanding of technology and thus enhance their ability to legislate intelligently about such issues. One underlying issue is a lack of resources: if legislatures want to be able to hire and retain

110 ibid.
111 See Linell Letendre, 'Lethal Autonomous Weapons Systems: Translating Geek Speak for Lawyers' (2020) 96 International Law Studies 274.
112 Deeks (n 109) 647.

technologically savvy staff, and conduct hearings that bring in a range of expert views on issues such as autonomous cyber tools, they need the funds to do so. In the United States, one think tank notes, 'Congress has simply not given itself the resources needed to efficiently and effectively absorb new information — particularly on complex [science and technology] topics'.[113] Others have advocated that the US Congress establish an internal body that is nimble, bipartisan and focused on providing options rather than recommendations.[114] Various European States have already established bodies that provide science and technology advice to legislatures; the United States could draw ideas from some of the different models represented there.[115] The European bodies should also ensure that they have experts at hand who understand machine learning and autonomous cyber systems, which will facilitate the legislators' ability to regulate such systems as they come online. Outside experts can be very useful here, both to educate legislatures and to surface and articulate competing views about the benefits and costs of this technology.

Legislatures should also consider setting up 'machine learning boot camps' for staffers who work on national security-related committees, to expose them to the basics of machine learning and cyber tools. Sessions run by outside tech experts who can present the information in clear, non-partisan, policy-relevant ways would be a helpful tool to ensure basic competence among policy and legal staff. In the United States, for example, Stanford University runs a 'Cyber and Artificial Intelligence Boot Camp' for congressional staffers. The boot camp draws on the experience of cybersecurity professionals, scholars, business leaders and lawyers to provide staffers with basic technical instruction, threat perspectives and exposure to simulated attacks.[116] Legislatures might also ask to observe actual testing and verification processes that take place inside the militaries, to understand how militaries decide that they have confidence in a particular autonomous system before deploying it.

2 *Updating Legislative Structures and Authorities*

In addition to raising their level of technological fluency, legislators should resist further erosion of their roles in overseeing the use of force and offensive cyber operations by updating their own ability to oversee

113 Miesen and others (n 91) 9.

114 Chris Tyler, 'Legislative Science Advice in Europe and the United Kingdom: Lessons for the United States' (*Lincoln Policy*) 8–9 <https://lincolnpolicy.org/wp-content/uploads/2020/02/TYLER.pdf>; Miesen and others (n 91).

115 Tyler (n 114).

116 Hoover Institution, 'Cyber and Artificial Intelligence Boot Camp' (August 2019) <https://www.hoover.org/events/cyber-and-artificial-intelligence-boot-camp-2019> accessed 14 October 2020.

cyber operations. One way to do this is to establish oversight committees dedicated specifically to cyber issues, as the recent Cyber Solarium project in the United States recommended. The Solarium report proposes that the US Congress create House and Senate committees on cybersecurity 'to provide integrated oversight of the cybersecurity efforts dispersed across the federal government'.[117] The committees, which presumably would draw their membership from existing armed services, intelligence and homeland security committees, could develop a deeper expertise on cyber issues — including the functions of autonomy in cyber settings — while building on their members' past experiences with war powers, use of force and technological questions.

Legislatures could also direct new regulatory efforts at autonomous cyber systems. For States in which existing statutes (rather than the constitution) allocate powers between the executive and legislatures, those legislatures should evaluate whether the statutes adequately reach cyber operations that either constitute or could quickly lead to international uses of force. In the United States, for example, the War Powers Resolution (WPR) creates a structure for executive consultation with and reporting to Congress before deploying armed forces into hostilities, but it quite clearly would not apply to the bulk of cyber operations, whether autonomous or not. One scholar has suggested amending the WPR to trigger the executive's notice requirement not only upon the introduction of troops but also upon the effectuation of military capabilities (such as cyber tools) in a situation that violates the sovereignty of another State.[118] This proposal might capture too many operations, however, especially if Congress's real interest lies in retaining some input into cyber operations that have the potential for escalation.

In any event, amending the WPR will be difficult, because the President would likely veto such changes. Thus, Congress would need to assemble a veto-proof majority that favors the bill.[119] But there may be more modest fixes that could achieve similar goals: in the United States, one adjustment might be to expand the list of committees that receive the forty-eight hour reports from the Defense Department under section 1642 of the 2019 NDAA.[120] That is, when the military has undertaken a 'sensitive military cyber operation' against Russia, China, North Korea

117 William Ford, 'The Cyberspace Solarium Commission Makes Its Case to Congress' (*Lawfare*, 18 May 2020) <https://www.lawfareblog.com/cyberspace-solarium-commission-makes-its-case-congress>.

118 Jensen (n 96) 553–54.

119 ibid (discussing legislative proposals to amend the War Powers Resolution).

120 2019 NDAA (n 75) § 1642; see also 10 USC § 395 (2019) (cross-referenced within § 1642).

or Iran, Congress should amend section 1642 to require that the military provide its written report not just to the armed services committees, but also to the intelligence and foreign affairs committees. Congress should also expand this notice requirement to cover sensitive military cyber operations against any State, not just these four States. Other legislatures should ensure that they are receiving adequate notice of significant cyber operations that implicate their regulatory and oversight powers.

Legislatures might also turn their attention specifically to the growing use of autonomous cyber tools, erecting guard rails around their use. Even if, as argued above, legislatures are not particularly well-suited to legislate in high-tech areas, legislatures should be able to navigate core legal and policy questions associated with autonomy.[121] First, legislatures should evaluate whether they are willing to accept their militaries' use of highly autonomous cyber tools generally. Some legislatures may accept the potential risks of such tools because they believe that the benefits are considerable. Others may not.

Second, those legislatures that accept in theory the use of autonomous cyber tools should define the basic contexts in which those tools are permissible, identify the adversaries against which the military may use the tools, define what kinds of foreseeable effects they are willing to tolerate, require the tools to be deployed in a way that is consistent with international legal requirements and require the executive to build in hard stops on escalation. Tim McFarland suggests, for instance, that a 'cyber weapon might be trusted to locate and identify potential targets autonomously, but be required to seek human confirmation before attacking them'.[122] The US Defense Department's Defense Innovation Board suggested that the department consider setting 'limitations on the types or amounts of force particular systems are authorized to use, the decoupling of various AI cyber systems from one another, or layered authorizations for various operations'.[123] Legislatures might fix in statute rules that require militaries to avoid uncontrolled escalation or impose the need for the effects of autonomous cyber operations to be reversible. They also could require that their executive branches only employ software in their cyber systems that is explainable or interpretable.

121 Liivoja, Naagel and Väljataga (n 14) 24.
122 McFarland (n 5) 33.
123 Defense Innovation Board, 'AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense Supporting Document' (US Department of Defense, 31 October 2019) 30 <https://media.defense.gov/2019/Oct/31/2002204459/-1/-1/0/DIB_AI_PRINCIPLES_SUPPORTING_DOCUMENT.PDF> .

At a more granular level, legislatures might take advantage of the fact that many cyber tools, even those that are increasingly autonomous, still require humans to carefully identify the tools' targets in advance and tailor those tools specifically to that threat. Even if legislatures have significant difficulties weighing in on hostile cyber operations close to the time at which the executive initiates those operations (including by unleashing a largely autonomous system), the legislatures could seek information from executive cyber operators about the pre-positioning efforts that the operators have undertaken to be able to launch operations in the future. Even if those pre-positioning efforts may primarily be to gather intelligence rather than to conduct an offensive operation, their dual-use nature means that legislatures would be within their rights to understand where and how their militaries or intelligence services are poised to initiate future cyber operations.

If a legislature is worried about its own abilities to substantively understand autonomous cyber tools and the risks that they pose, it could establish a commission of independent experts — with appropriate security clearances — to review, analyze and report on executive branch conduct involving relevant technologies. Such a commission might examine compliance with both international and domestic law, and could report regularly to legislatures and, in an unclassified form, to the public. Precedent for these types of bodies include the Privacy and Civil Liberties Oversight Board in the United States and the Investigatory Powers Commissioner in the United Kingdom.[124]

Finally, legislatures should impose reporting requirements on executives so that legislators are aware of the types of autonomous cyber systems their militaries are using and what effects the systems are producing or have the capacity to produce. They might even require reports from foreign ministries on the foreign policy implications of any autonomous cyber operations that occur, thus ensuring that those ministries retain visibility into those operations.[125] These steps will help preserve a level of democratic accountability for uses of force or other escalatory cyber actions.

124 Joanna Dawson and Samantha Godec, 'Oversight of the Intelligence Agencies: A Comparison of the "Five Eyes" Nations' (House of Commons Library Briefing Paper No 7921, 15 December 2017) <https://commonslibrary.parliament.uk/research-briefings/cbp-7921/>.

125 In the US statute creating the Global Security Contingency Fund (the FY 2012 National Defense Authorization Act), Congress required a form of 'dual-key' authorization and reporting, whereby decisions about funding are made jointly by the Secretaries of State and Defense, and those agencies send reports jointly to multiple committees. Nina Serafino, 'Global Security Contingency Fund: Summary and Issue Overview' (Congressional Research Service Report No R42641, 4 April 2014) <https://fas.org/sgp/crs/row/R42641.pdf>.

B SECURING EXECUTIVE BALANCING AMONG AGENCIES

Legislators are not the only actors whose input may be threatened by increasingly autonomous military tools. As Part IV discussed, the operation of highly autonomous cyber tools might diminish the opportunities for civilian officials within the executive branch to provide input into activities that could produce major foreign policy consequences. Because the cyber tools that will perform these autonomous operations will be constructed in advance, however, there is an opportunity for a range of relevant agencies to provide input into the parameters of those systems. One way to do this is to establish standing rules of engagement to guide how the military deploys the systems, and to craft those rules of engagement through an interagency process.[126] This would give civilian officials insight into and influence on the ways that the military uses advanced autonomous cyber systems.

Even if interagency officials such as diplomats, career analysts and civilian national security lawyers are not directly engaged in crafting military rules of engagement, there is still room for interagency participation in developing the rules of the road for use of autonomous cyber tools. Two scholars recently noted, 'Insights from the literature on civil-military relations and planning suggest not leaving cyber strategy to soldiers alone'.[127] They add, 'There are major questions regarding how to craft a policy framework for cyber strategy that does not create dangerous escalation pathways or jeopardize civil liberties and the free flow of information. These questions should not be reduced to expediting authorities at the expense of interagency coordination or civilian oversight'.[128] These scholars propose developing 'flexible response options precleared to balance equities and assess risks', which would ensure 'time-sensitive responses without sacrificing interagency coordination'.[129]

126 Erica Borghard and Shawn Lonergin, 'What Do the Trump Administration's Changes to PPD-20 Mean for US Offensive Cyber Operations?' (*Council on Foreign Relations*, 10 September 2018) <https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations> (noting that 'some risks [that attach to loosening interagency control over cyber operations on the tail end] can be mitigated through developing standing rules of engagement' that could 'mitigate some concerns about escalation' and that the process of establishing the rules of engagement could codify and address those concerns).

127 Benjamin Jensen and JD Work, 'Cyber Civil-Military Relations: Balancing Interests on the Digital Frontier' (*War on the Rocks*, 4 September 2018) <https://warontherocks.com/2018/09/cyber-civil-military-relations-balancing-interests-on-the-digital-frontier/> (arguing that letting soldiers plan in isolation produces 'narrow plans prone to escalation risks', leads to 'false optimism [and] overconfidence', and 'diminishes the probability of successful, coercive diplomacy').

128 ibid.

129 ibid.

The need for militaries to respond in a timely way is a real one; disorganized interagency processes can hinder that. Under the Obama Administration, the United States used an interagency cyber process that often got bogged down in infighting.[130] Its 'interagency de-confliction process suffered from delays, bureaucratic inertia, ill-defined decision pathways, and the lack of a clear "referee" to resolve competing positions at the working level'.[131] For example, there was a 'fierce debate' among different executive agencies about whether to notify States hosting computer services used by ISIS that the United States planned to sabotage those services, a dispute that took weeks to resolve.[132] The Trump Administration modified the interagency process, apparently delegating far more decisions about offensive cyber operations to military commanders and decreasing interagency input. Further, the Trump Administration seems to have authorized the CIA to undertake covert offensive cyber operations against several adversaries, and to do so with a new level of independence from the White House.[133]

Because the Trump policies and the subsequent operations under them remain classified, it is unclear whether these policies have produced better or worse results from a US foreign policy perspective.[134] In any event, developing an executive process that adequately balances the need for effective military cyber responses against harm to diplomatic, law enforcement and intelligence cooperation may take time and multiple iterations to get it right. In the United States, there is a debate, for example, about whether to create a 'National Cyber Director' to coordinate those responses or whether to rely on the National Security Council to do so.[135] Regardless of the specific mechanisms they use, States must

130 ibid.
131 ibid.
132 Ellen Nakashima, 'US Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies' (*Washington Post*, 9 May 2017) <https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html>.
133 Zach Dorfman and others, 'Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks' (*Yahoo News*, 15 July 2020) <https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html>.
134 David Kris, 'What Hard National Security Choices Would a Biden Administration Face?' (*Lawfare*, 27 May 2020) <https://www.lawfareblog.com/what-hard-national-security-choices-would-biden-administration-face> ('A Biden administration will need to understand … exactly how much power to act now resides in military commanders; and how much interagency coordination is required before action can be taken. It might want to adjust protocols in favor of less delegation, particularly at the beginning of the administration when new officials are less aware of and comfortable with the precedents and understandings developed in the Trump administration'.); Eric Geller, 'Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand' (*Politico*, 16 August 2018) <https://www.politico.com/story/2018/08/16/trump-cybersecurity-cyberattack-hacking-military-742095> (discussing pros and cons of the interagency process under the Obama administration).
135 Philip R Reitinger, 'Establishing a National Cyber Director Would Be a Mistake' (*Lawfare*, 17 July 2020) <https://www.lawfareblog.com/establishing-national-cyber-director-would-be-mistake>.

preserve important elements of civilian control and oversight over autonomous military cyber operations as they try to strike the proper balance among their various security and foreign policy equities.

Just as legislative staff should improve their cyber literacy, so too should executive officials who work on cyber issues. Governments could detail national security lawyers in foreign, justice and intelligence ministries to technology offices in their own or other agencies. They could also detail cyber experts to policy positions, such as to positions in NATO or in their foreign ministries. This would have to be done in a way that rewards these officials for taking these non-traditional postings, along the lines of the requirement in the US Goldwater-Nichols Act that requires joint-duty assignments for military officers seeking career advancement. Further, like legislative staffers, executive agencies should mandate that those civilian officials who work on cyber and technology policy issues attend machine learning and cyber bootcamps to establish basic familiarity with those tools and their future prospects.

These measures, which would provide a form of internal checks and balances among different executive agencies, should improve the quality of executive decision-making. As I noted elsewhere:

> Particularly in the national security area, where Congress and the courts face institutional and structural challenges to providing robust oversight, it has become commonplace to turn to checks within the executive branch itself as an alternative to inter-branch checking. The inter-agency policy-making process requires — and indeed benefits from — exchanges among different executive agencies with distinct mission statements. Each agency pursues its own goals and policies, while trying to avoid policies that undercut the agency's mission or unduly weaken its standing in relation to other agencies.[136]

It therefore seems healthy to ensure that a range of civilian agencies and officials retains a role in shaping the use of highly autonomous cyber tools. This is particularly true because it may be hard for legislatures to serve in their constitutional checking role in relation to these tools. Cyber autonomy may be critical at the moment of an attack, but there is ample room in advance to shape that autonomy's characteristics and uses.

136 Ashley Deeks, 'A (Qualified) Defense of Secret Agreements' (2017) 49 Arizona State Law Journal 713, 776.

C ROLES FOR ALLIES AND OTHER EXTERNAL ACTORS

This article suggests that a range of States face some shared challenges when it comes to democratic accountability for the use of cyber autonomy. As a result, there may be value in sharing experiences among executive and legislative branches of NATO member States. Understanding how allied counterparts approach regulatory issues, deficiencies in technological knowledge and legal questions raised by highly autonomous military operations could produce creative ideas about ways to preserve and even bolster democratic accountability. Close allies might even consider sharing detailed information about their own autonomous systems, to identify and troubleshoot international legal issues.

Another source of constraint on executive actors undertaking classified national security operations, such as cyber operations, is US technology and cybersecurity companies. In some settings, these companies have incentives to check poor executive decision-making that happens behind the veil of classification. These actors often have access to incoming cyber threats, have independent tools by which to attribute attacks and have the expertise to observe and critique certain US government cyber operations.[137] The US Congress might do well to harness these 'surrogates' as information-gatherers and a source of technological expertise about the growing autonomy of cyber operations by the United States and other States.

VI CONCLUSION

Highly autonomous cyber operations are near at hand. Even if States manage them very carefully, the potential exists for States to engage in unintended cyber hostile acts that might lead to armed conflict. At least in democracies, legislatures have historically had a role to play in checking executive branch military and foreign policy decisions, even if that role today is increasingly narrow. Both legislatures and executives have a responsibility and an opportunity to establish appropriate parameters for

137 Deeks (n 84) 145–46.

the use and oversight of autonomous cyber weapons. These parameters should preserve input from a range of knowledgeable actors and thus ensure that democratic accountability and other public law values, such as competence and legal compliance, are preserved in States' autonomous cyber operations.