A Transatlantic Dialogue on Military Cyber Operations
Amsterdam, August 13, 2019
Workshop Report

Conveners:
Robert M. Chesney, The University of Texas at Austin
&
Max Smeets, ETH Zurich

Rapporteur
Monica Kaminska, University of Oxford

General Overview

On August 13, 2019, the Strauss Center for International Security and Law at The University of Texas at Austin and Stanford University's Center for International Security and Cooperation (CISAC) convened a workshop to discuss American and European military cyber operations. The event gathered leading experts from military, civilian, and academic institutions. Its overall aim was to gain a sharper understanding of the changes in cyber policy and practice introduced across the Atlantic.

The workshop was structured around five panels:
- Panel 1: The European Policy Landscape
- Panel 2: The US Strategy of Persistent Engagement and Defend Forward
- Panel 3: Assessing the Risks Involved in Implementing Changes in Strategic Doctrine
- Panel 4: The Procedures and Implications of Out-of-Network Operations in Allied Networks
- Panel 5: Avenues for Coordination and Cooperation amongst Allied Countries

This report summarises the workshop proceedings. For each panel discussion, it describes the topics of discussion, summarises the main points made, and provides recommendations for policy action or further enquiry.

For more information on this publication: Please contact Robert Chesney, rchesney@law.utexas.edu or Max Smeets, msmeets@ethz.ch

For Academic Citation: Kaminska, Monica, Robert Chesney, and Max Smeets. "A Transatlantic Dialogue on Military Cyber Operations." Workshop Report, University of Texas at Austin, Amsterdam, August 13, 2019

Panel 1: The European Policy Landscape

A. Topic Description

This panel discussion explored changes in thinking and concepts, in particular theoretical, doctrinal, and legal frameworks, for the governance of military cyber operations within the Atlantic community. Questions explored included the following:

- What are different governments' main objectives behind their cyber strategies?
- How do they seek to accomplish these objectives?
- What means currently exist to pursue them?
- What changes in cyber strategy and implementation are expected in the near future?

A central point of the discussion was defining the scope of the military's role in cyberspace within different national jurisdictions. The time for such discussions could not be more opportune: governments are increasingly sharpening and revealing their cyber strategies. For instance, France published its military cyber strategy for the first time in January 2019.[1] France's *Commandement de la cyberdéfense* (COMCYBER), which has existed since January 2017, operates under the direct authority of the chief of the defence staff.[2] Similarly, the Dutch government published, in 2018, its Defence White Paper promising to invest in the development of cyber capabilities to improve the government's ability to execute defensive and offensive activity.[3] Already in 2014 the country had established its Defence Cyber Command (DCC) within the Ministry of Defence.[4] Estonia, in 2018, launched the Defence Forces' cyber command with the expressed purpose of conducting active cyber defence operations – a major leap for the country that a decade earlier had published the world's first national cyber strategy.[5]

B. Summary of Main Points

The discussion revealed notable differences among national conceptions of cyber defence – in particular the French, Dutch, and Estonian conceptions. Let us begin with the French approach.

---

[1] Ministère des Armées, 'Discours de Florence Parly, ministre des Armées, Stratégie cyber des Armées.', 18 January 2019, https://www.defense.gouv.fr/salle-de-presse/discours/discours-de-florence-parly/discour-de-florence-parly-ministre-des-armees-strategie-cyber-des-armees.

[2] François Delerue, Alix Desforges, and Aude Géry, 'A Close Look at France's New Military Cyber Strategy', War on the Rocks, 23 April 2019, https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/; Stéphane Taillat, "Signaling, Victory, and Strategy in France's Military Cyber Doctrine", War on the Rocks, May 8, 2019, https://warontherocks.com/2019/05/signaling-victory-and-strategy-in-frances-military-cyber-doctrine/

[3] Ministry of Defence, The Netherlands, '2018 Defence White Paper Investing in Our People, Capabilities and Visibility', 2018, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjMsqaa3NfkAhXOXRUIHb7yC2MQFjAAegQIAxAC&url=https%3A%2F%2Fenglish.defensie.nl%2Fbinaries%2Fdefence%2Fdocuments%2Fpolicy-notes%2F2018%2F03%2F26%2Fdefence-white-paper%2FDefence%2BWhite%2BPaper%2B2018.pdf&usg=AOvVaw1pPtgzFVKj3DpyLtC2QiT3.

[4] Alexander Claver, 'Governance of Cyber Warfare in the Netherlands: An Exploratory Investigation', *The International Journal of Intelligence, Security, and Public Affairs* 20, no. 2 (4 May 2018): 155–80, https://doi.org/10.1080/23800992.2018.1484235.

[5] 'Estonian Cyber Command: What Is It For?', ICDS, accessed 17 September 2019, https://icds.ee/estonian-cyber-command-what-is-it-for/.

French cyber doctrine consists of four notable elements. One is a peculiarly French notion of cyber defence (*ciber defence*) that differs from the Anglo-Saxon one, because its objective is less about defending networks – the American and British priority – and more about ensuring that the government and the military are able to function in times of crisis. Crucially, despite the "defence" label, in order to achieve this objective, the strategy accepts the necessity of operating offensively rather than purely defensively – a point of similarity with the American notion of "active defence". The propose of offensive activity, however, is not merely protecting the functionality of vital infrastructures. It is also about monitoring the operational space. French doctrine recognises the dangers to the stability of international interactions inherent in this approach, which it seeks to reduce.

A second main element of French doctrine is "strategic autonomy" – a notion that is gaining credence within European Union cybersecurity circles.[6] It captures the French government's desire to retain its native capacity for strategic analysis, particularly in times of crisis. Here, then, a central theme of French doctrine re-emerges: the retention of national autonomy for meaningful action in the midst of a crisis, however dire. For this reason, the French government does not normally engage in public attribution, because divulging an attacker's identity risks limiting the freedom of action if military and intelligence services in the selection of a response. There are also political reasons for France's reluctance to attribute, namely the desire to maintain independence from US and NATO thinking, and bureaucratic incentives. France's reaction to the cyberattack on TV5Monde exemplifies its approach: while the government strongly signalled that it was not willing to engage in public attribution, and indeed never issued an attribution statement, it also indicated that it was fully aware of the perpetrator's identity and had deep knowledge of the operation. The French government's reluctance to engage in collective attribution has also led to accusations that it is free riding on the attribution conclusions of private sector companies.

Third is France's organisational approach. It allocates responsibility for cyber operations between the aforementioned COMCYBER, which is tasked with offensive activity; the Ministry of Defence, which is responsible for cyber defence more broadly; and the National Cybersecurity Agency (ANSSI) within the Prime Minister's Office that protects governmental networks.[7]

Fourth is France's unique position on the question of sovereignty as a "rule" in cyberspace. As clarified by the French Ministry of Defence in September 2019 document explaining France's application of international law in cyberspace, a hostile cyber operation launched by another state against French cyber infrastructure violates French sovereignty from the moment at which there is a penetration of French computer systems.[8] In other words, according to France, a violation of international law occurs even *before* tangible effects are produced within French territory.[9]

---

[6] Paul Timmers, 'Strategic Autonomy and Cybersecurity', Policy in Focus (EU Cyber Direct, May 2019), https://eucyberdirect.eu/wp-content/uploads/2019/05/paul-timmers-strategic-autonomy-may-2019-eucyberdirect.pdf.
[7] Delerue, Desforges, and Géry, 'A Close Look at France's New Military Cyber Strategy'.
[8] Ministére Des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace', 9 September 2019, https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf.
[9] Przemyslaw Roguski, 'France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I', *Opinio Juris* (blog), 24 September 2019, https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/.

In sum, in the French conception, offensive activity seeks to generate an effect against an adversary, while defensive activity aims to preserve freedom of action in pursuit of strategic autonomy – an overarching principle of France's defence doctrine – all the while observing different competences among military and civilian government bodies.

The Dutch perspective also emerged during the discussion. It differs from the French one in its emphasis on the value of collaboration and consensus building, which is particularly visible in the Dutch government's willingness to publicly attribute attackers multilaterally. Another central feature of the Dutch approach is its special focus on developing international norms of cyber attribution. As part of this objective, it endeavours to raise the general public's awareness of states-based cyber threats.

The new Dutch cyber agenda presents a risk-based identification of digital national interests, which includes determining what assets need protecting, what the threats are, and what actions need to be taken. Recent efforts in this direction have involved telecommunications providers and included an assessment of the challenges associated with the security implications of 5G infrastructure. There is also a recognition that it is necessary to simulate crisis situations that test existing response procedures. In addition, the Dutch government recognises the need to work extensively with the private sector entities, many of which have been experimenting with the development of self-defence capabilities of their own. The government's defence white paper showed that the Netherlands places a special emphasis on the role of the military in cyberspace in an effort to develop their own version of "forward defence".

Estonia presented another national approach. While the country established a national cyber command only recently, its voluntary cyber defence unit (*Küberkaitseliit*) has existed since 2011. Notably, moreover, Estonia was the first country to publish (in 2008) a national cyber defence strategy, the necessity for which became evident during the cyberattacks that interrupted financial and governmental communications systems the previous year.

The Estonian approach to cyber strategy gives special importance to NATO. As one of only seven nations that fulfil the alliance's minimum defence spending obligation of 2% of GDP,[10] Estonia has committed both defensive and offensive capabilities to the alliance as well as regularly organising and hosting its joint exercises (e.g. "Locked Shields"). Another priority is crisis preparedness – that is, enhancing the response to a 2007-type incident. This concern for defence over offence – perhaps natural for a small nation lacking the resources for major operations – is reflected by the raison d'être of the cyber command, which is to streamline disjointed organisations to improve defensive responses, rather than to enhance attack capabilities (as in the United States).

Another purpose of the command is the improvement of inter-allied cooperation, particularly in the area of intelligence sharing. Here, a difference emerges in comparison to the Dutch cyber strategy: while the Dutch seek to develop offensive capabilities to strengthen deterrence, the Estonians preferred approach to conflict prevention focuses on allied collective defence. Nevertheless, the 2019-2022 Estonian cybersecurity strategy asserts the

[10] 'Seven NATO Countries Hit Spending Target', France 24, 14 March 2019, https://www.france24.com/en/20190314-seven-nato-countries-hit-spending-target.

goal of developing cyberattack capabilities (including within the military conscription service).[11]

In sum, the Estonian cyber strategy emphasises four areas of activity:

- Establishing real time cyber situational awareness across the civilian and military sectors
- Developing cyberattack capabilities
- Creating a cyber capacity within the conscription service
- Enhancing regional and international coordination to facilitate attribution of attacks, strengthen deterrence, and improve international stability

C. Recommendations for action or further enquiry

The discussion raised an important question about the utility of distinguishing between offence and defence in the cyber domain. The reality of activities in this space, for example threat hunting outside of home networks, is so fluid that it may not make sense to distinguish between offensive and defensive activity. At the same time, the participants recognised that this distinction will likely persist because of national bureaucratic and institutional structures and their missions.

[11] Ministry of Economic Affairs and Communications, 'Cybersecurity Strategy Republic of Estonia', 2019, https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

Panel 2: The US Strategy of Persistent Engagement and Defend Forward

A. Topic Description

The panel's objective was to explore the means and ends of "persistent engagement" and "defend forward". The following questions were explored (among others):

- What are the USG and US CYBERCOM objectives in cyberspace?
- How does USG AND US CYBERCOM aim to accomplish its goals?
- What are the means required to enable and execute defend forward and persistent engagement?

B. Summary of Main Points

The discussion first recognised the realities of the strategic space, its interconnected structure and the condition of constant contact, and surveyed developments in US policy as reflected in conceptual shifts during the last three years. From 2011 until 2016, US cyber strategy adhered to a doctrine of restraint and a strategy of deterrence, in which the main objective was to shift the decision calculus of the adversary. This emphasis no longer holds sway following the introduction of Defend Forward and Persistent Engagement into the strategic lexicon in 2018.[12] Defend Forward is the cornerstone of the 2018 cyber strategy of the Department of Defense, which is operationalised by US Cyber Command through the associated strategy of persistent engagement. The discussions revealed the significant progress made in recent years and the lag in the wider adoption of these new concepts across the national security enterprise. One of the rationales of the Cyberspace Solarium Commission is to address this wider adoption.

A second major point of discussion focused on the outcome variable of success in a persistent strategic environment: How do you measure the efficacy and success of persistent engagement and Defend Forward? Whereas from 2011 to 2016 the focus of deterrence strategy was on altering the adversary's decision calculus, this emphasis does not make sense in an environment of persistent engagement. The adversaries' calculus is a given: they are expected to persist.[13] Discussions revealed that the chief measure of success is changing the conditions of security – not the adversaries' calculus.

Under a persistent engagement model, success is achieved through continuous operations that anticipate the exploitation of the adversaries' and one's own vulnerabilities. The question becomes: Can you anticipate how you will be exploited and will you be in a position to exploit the vulnerabilities of others? So the objective then becomes: Who has the balance of initiative? The objective for the United States, therefore, becomes shifting the balance of initiative in its favour. Once this is done, the United States is then able to set the conditions of security. Upon gaining the initiative, the United States is able to effectively structure the

---

[12] US Cyber Command, 'Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command', 2018, https://assets.documentcloud.org/documents/4419681/Command-Vision-for-U.S. Cyber Command-23-Mar-18.pdf; U.S. Department of Defense, 'Cyber Strategy', 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEG Y_SUMMARY_FINAL.PDF.

[13] Also see: Fischerkeller, Michael P., and Richard J. Harknett. "Deterrence is Not a Credible Strategy for Cyberspace." Orbis 61, no. 3 (2017): 381-93. https://www.sciencedirect.com/science/article/pii/S0030438717300431

playing field – not just for itself but also for its adversaries. US adversaries are then forced to play on a field that is better suited to US strengths.

Persistent engagement, however, should not be seen as aggressive or offensive. Instead, it should be conceived of as a more active strategy whose intent and tactics are primarily defensively oriented. This also means that Defend Forward should not be seen as pre-emption, that is, actions to prevent imminent attack. Rather, the intention is to compete more effectively below the threshold of armed conflict. Crucial is the recognition that it is possible to engage in defensive operations outside your own network, and the need to contest and counter adversarial campaigns as close as is practicable to the source of activity before they breach our networks.

Two examples of the new strategy in practice are the takedown of the Russian Internet Research Agency as part of a campaign to protect the 2018 US mid-term elections and the upload of files identified by US Cyber Command as malicious to Virus Total. The latter has also been a means of leveraging a different relationship with the private sector.

A third topic that featured prominently in the discussions was an assessment of the current geostrategic environment. The United States is now concerned with grand strategic competition. While Britain in the late nineteenth century was an economic rival, China is not only an economic but also a strategic competitor. The challenge from Russia is altogether different; the Putin government appears more interested in the manipulation of the information space and disruptive campaigns that delegitimize democratic institutions, sow discord in American society, and undermine alliance cohesion. Perhaps most significantly, the majority of geostrategic competition is being played out below the level of armed attack. Adversaries are able to degrade sources of national power without resorting to armed attack. This is something that has become possible through the expansion of the interconnected cyber strategic environment.

Consider the example of the 2015 Bangladeshi central bank heist, which North Korea perpetrated to compensate for the robust economic sanctions regime levied by the United States. In order for North Korea to have executed the same heist using non-cyber means it would have had to deploy an entirely different force and capability, most likely using armed force. This new reality presents a policy conundrum, because for decades the United States organised itself strategically to manage strategic outcomes through coercion and the threat of war.

C. Recommendations for Action or Further Enquiry

The discussion raised the important question: To what degree should the defence of mostly private networks be regarded as a military (as opposed to a civilian) activity? Related to this is the question of how “cybersecurity” should be defined. Does the notion extend to disinformation campaigns and the protection of pollsters as opposed to just the protection of electoral systems and the integrity of data? Is this information space even defensible?

Another issue that the discussion identified as meriting special attention is the possibility of intelligence agencies losing elements of their offensive toolkits. Such an incident occurred, for instance, in 2013 when a group calling itself the Shadow Brokers released valuable NSA intrusion tools online. Discussants noted that the difficulty of securing exploit kits and the potential of inadvertently arming adversaries through the kits’ proliferation is a question deserving policymakers’ serious attention.

Panel 3: Assessing the Risks Involved in Implementing Changes in Strategic Doctrine

A. Topic Description

The panel explored the following questions:

- What are the risks to the United States and its allies of implementing U.S. Cyber Command strategies on the other side of the Atlantic?
- What are the risks of *not* implementing it?
- To what degree does US cyber strategy risk conflict escalation between the United States and its main adversaries?

B. Summary of Main Points

The starting point of the discussion involved an important recognition: cyber attacks should seen not as isolated events, but rather as elements of larger campaigns. Examples of such campaigns include Russia's efforts to destabilise Western democracies, China's intellectual property theft, and Iran's efforts to sow political disruption in the Gulf region. In order to counter these campaigns, we should implement "campaign" thinking in cyberspace ourselves, for which we must engage all the tools of national power – the so-called Whole of Nation approach. This is largely consistent with the current US government's approach to cyberspace, especially as reflected in Persistent Engagement. While Persistent Engagement entails significant risks for America, its allies, and conflict stability, the panellists debated whether it could be less risky than the previous approach of inaction.

The discussion then proceeded to an identification of the risks associated with Persistent Engagement. One is escalation: if an adversary misunderstands an action or operation and responds in a way that is perceived as disproportionate, a spiral of retaliation could ensue, leading to eventual conflict. At the same time, inaction itself eventually also carries the same risk. If a state does not respond punitively to cyber campaigns, then it effectively signals to its adversaries that their hostility is an acceptable form of behaviour. The consequence off such initial restraint is that in the future the state might not be able to respond to the same actions under international law, which may also lead to conflict. A further consideration is that adversaries prefer to avoid escalation if they can. Hence, while it is important be mindful of the risks of spiraling conflict, their consideration should not be overblown.

A second risk is distraction: by focusing on Persistent Engagement, the United States risks detracting from planning for conflict and crisis. Moreover, the United States may "burn" its capabilities during Persistent Engagement, thereby leaving a depleted toolbox for a conflict situation. Thus, it is critical that the government maintain tools and capabilities that would allow it to respond to an attack on critical infrastructure, while at the same time engaging persistently. Here emerges a third risk: after capabilities are used or 'burned', their revealed features enable adversaries to potentially copy or emulate them.

Isolation presents a fourth risk. The United States may find it difficult to convince its allies that the new strategy entails a reasonable and appropriate set of responses that others will implement responsibly or effectively. Policymakers should pay particular attention to the effects Persistent Engagement has on the dynamic of US alliances – a cornerstone of US

security. The discussants acknowledged, however, that when used adaptively and wisely, Persistent Engagement can potentially bolster relationships between allies.

Another focus of the discussion was the trade-off between increasing the security of cyberspace in general – for example, by a government entity disclosing vulnerabilities to private vendors – and the benefits that holding such vulnerabilities in secret could bring for government cyber operations. The panel made the point that the stability of cyberspace is more important than a single nation holding superior capabilities. Persistent Engagement should therefore be implemented in such a way that the goal of creating a stable and secure cyberspace has a bearing on the type of operations that the state chooses to engage in.

The panel also proposed a systems theory approach to looking at Defend Forward and Persistent Engagement. It asked: Is Defend Forward and Persistent Engagement going to magnify positive or negative feedback loops?[14] A positive feedback loop occurs when an initial signal is amplified, resulting in system instability. An example of such an effect would be if other nations were to react in a "tit for tat" manner and retaliate against cyber activity. A negative feedback loop counters a stimulus, readjusting the system back to a state of equilibrium. The friction created by Persistent Engagement is an example of this: the imposition of costs will directly frustrate adversary operations.[15] The panel concluded that it is not yet clear whether Defend Forward and Persistent Engagement would generate more negative or positive feedback loops. The concern is that positive feedback can be generated by a number of features unique to the cyber domain. These are the following: first, the severity of the security dilemma is increased in cyberspace because it is not known whether the weapons that are being acquired by the other side are defensive or offensive in nature.[16] Second, these capabilities are not just being stockpiled by nations, they are being used. Finally, the playing field is not just limited to two actors, but multiple actors. Since the answers to these questions are not yet known, the current situation is one of trial and error. This gives reason for significant caution when introducing new operational frameworks.

Finally, the discussion turned to whether Persistent Engagement is an appropriate for dealing with all types of cyber actors and cyber campaigns. The strategy has clear benefits for dealing with Russia whose chief cyber campaigns is an information campaign. Imposing friction over a sustained period of time can be an effective strategy for countering such activity. In the case of Chinese espionage campaigns, however, it will likely be far more difficult to derail, through friction, an already mature organisational machinery that is concerned solely with tool development.

C. Recommendations for Action or Further Enquiry

The discussants agreed that any actions that fall under Persistent Engagement should be undertaken in such a way that they are legitimate and publicly defensible, both in the eyes of domestic publics and from the perspective of US allies – in other words, actions have to be

---

[14] For a more detailed discussion also see: Jason Healey, "The implications of persistent (and permanent) engagement in cyberspace," *Journal of Cybersecurity,* 5:1(2019); The language of 'positive' and 'negative' feedback loops might be confusing, as a 'positive feedback' leads to potentially negative implications, and vice versa.

[15] Robert Jervis and Jason Healey, 'The Dynamics of Cyber Conflict', *Columbia SIPA*, 2 August 2019, 1–4.

[16] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations* (London: Hurst & Company, 2016).

consistent with the norms and rules of International Law. The recommended course of action is to pay attention to the types of campaigns and actors that Persistent Engagement and Defend Forward might be best at countering, while maintaining an eye on possible positive feedback loops.

Panel 4: The Procedures and Implications of Out-of-Network Operations in Allied Networks

A. Topic Description

This panel turned specifically to allied networks in search of answers to the following questions:

- What are the current procedures for U.S. Cyber Command to conduct out-of-network operations?
- What are the incentives for U.S. Cyber Command to achieve effects outside of 'blue space'?
- What are the implications of U.S. Cyber Command operating "globally, continuously and seamlessly" for its allies?

B. Summary of Main Points

The first focus of the discussion were the legal and policy changes in the United States that underpin or constrain out-of-network operations.[17] The National Defence Authorisation Act (NDAA) gradually introduced notable legal changes in this direction, but the past year saw the biggest set of changes to the oversight and authorisation architecture. Three changes are most prominent. Firstly, the changes confirmed that the Department of Defense has authority to operate in the cyber domain outside of the context of defending its own networks. Secondly, they clarified when the executive can decide on the undertaking of operations outside US territory without Congressional authorisation. Congress explicitly set out the following conditions for U.S. Cyber Command to engage in offensive activity below the level of armed conflict:

- The activity has to be conducted in response to systematic ongoing action affecting US national interests, particularly election interference.
- The activity has to be first attributed to one of the so-called Big Four: Russia, China, North Korea, or Iran.

Thirdly, Congress explicitly articulated that the activity conducted by U.S. Cyber Command does not constitute "covert action" as defined by US domestic law. This was perhaps the most important clarification, because such a definition would trigger a well-established covert action framework, which includes gaining presidential authorisation for such activity and reporting to the Congressional intelligence committees, rather than the armed services committees. Defining cyber operations as covert action could raise questions as to whether the CIA, rather than U.S. Cyber Command, ought to be the agency responsible for their delivery. Congress has also created an oversight framework for military cyber operations, which requires that activities are reported to the armed services committees.

---

[17] For an overview also see: Chesney, Robert. "CYBERCOM's Out-of-Network Operations: What Has and Has Not Changed Over the Past Year?", Lawfare , May 2019, https://www.lawfareblog.com/cybercoms-out-network-operations-what-has-and-has-not-changed-over-past-year; Chesney, Robert. "The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes", Lawfare, 2018, September 25, https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defenseforward-light-ndaa-and-ppd-20-changes

The general conclusion that can be drawn from the policy changes is that U.S. Cyber Command can now be more efficient in conducting its operations because it is no longer required to consult the White House or undertake the inter-agency process as frequently as before.

A second focus of the discussion was the implications of Persistent Engagement and Defend Forward for US allies.[18] For years, the United States has operated in allied networks for the purposes of fourth party intelligence collection; and also by passing through allied networks to gain access to adversary space. The new operational strategy set out by the Department of Defense, however, implies that the United States intends to become a disrupter, operating beyond its networks and as close to the source of cyber activity.[19] This is likely to mean operating within allied networks. Thus far only one example of such activity exists: an operation where the United States took over an Islamic State server based in Germany, but without notifying Berlin prior to the operation – thereby reportedly creating tension between the two allies.[20] By operating in networks that are likely to be a hotbed of intelligence collection by other states' intelligence agencies, the United States could risk uncovering its allies' operations and even burning their toolsets. Thus, the new DoD strategy may prompt allied nations' intelligence agencies to change their operational procedures. The discussion also identified a related risk. Countries like Russia are known to exploit inter-allied friction for their own strategic benefit. It is conceivable, therefore, that adversaries will choose to operate within allies' networks in order to divide them.

A further consideration is how the strategy of Persistent Engagement can be independently adopted by different countries. The prospect is not difficult to imagine: the reality of security within an environment of constant contact may lead other nations to pursue their own version of Persistent Engagement – indeed, there are already indications that the United Kingdom is leaning in this direction.

It is not immediately clear, however, that Persistent Engagement can be implemented in different countries in a way similar to deterrence strategy. At the same time, the integration of other countries' strategies of Persistent Engagement would clearly benefit US interests – if, for example, it prompted other nations to collaborate with the United States in identifying and uploading malware samples to Virus Total.

C. Recommendations for Action or Further Enquiry

In order for Persistent Engagement to be implemented successfully across other nations, the discussion distinguished two main areas requiring further elaboration:

- The language around "territory" should be made clear. What does the United States consider the source of cyber activity to be: the router, the server, or where the malware is developed? How does the United States distinguish between "red space"

[18] Also see: Smeets, Max. "Cyber Command's Strategy Risks Friction with Allies." Lawfare , May 28, 2019. https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.
[19] United States of America Department of Defense, 'Summary: Department of Defense Cyber Strategy 2018', 2018, https://bit.ly/2JcOwFr.
[20] Ellen Nakashima, 'U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies', *Washington Post*, 9 May 2017, sec. National Security, 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.

and “grey space”?[21] What red lines does the United States see in this operational environment?

- There should be more focus on the relationship between Defend Forward and Persistent Engagement. To what degree is Defend Forward necessary for the success of Persistent Engagement? Do the inherent characteristics of cyberspace require a Defend Forward approach?

Another idea put forward in the discussion is the creation a coordinated notification equity process for out-of-network operations. Such a framework would serve to increase trust between the United States and its allies. Specifically, it would establish communications procedures for the United States to inform its allies of planned operations within their networks. By sharing such procedures broadly, the United States would send a clear signal that there exists a clear process of consideration prior to engagement. Even if such communications channels already exist, it would be beneficial to insert them into a clear, formal framework that can be widely communicated among allies.

Panel 5: Avenues for Coordination and Cooperation amongst Allied Countries

A. Topic Description

The final panel delved deeper into the topics raised in the preceding panel by exploring the following questions:

- What are the avenues for coordination and cooperation amongst allies?
- What is NATO’s role in promoting international coordination and cooperation?

B. Summary of Main Points

The panel examined the prospects for cooperation and collaboration through partnerships. States and militaries acting alone are often unable to marshal the capital, manpower, and knowledge to conduct cyber operations successfully. International partnerships could address this limitation: by combining their offensive cyber capabilities, states can overcome the demanding operational requirements of cyberspace in terms of presence, reach, and the maintenance of an advantage. The aim of partnerships, then, is a multiplication and cost reduction effect. In this way, paradoxically, joint efforts enhance states’ ability to exercise their national sovereignty in a complicated domain.

The necessity for partnerships in cyberspace also arises from the domain’s character – namely, its constant global interconnectivity. In order to generate full-spectrum cyber effects, it is therefore necessary to move beyond simple ideas of coordination and cooperation between militaries, states, and the private sector; one must also consider how to generate integrated activity that is delivered through common operational effect among diverse actors.

Meaningful partnerships are fundamental to enhancing military ability to manoeuvre in cyberspace. Specifically, four partnership dimensions stand out. First are “partnerships of influence”, which, as discussed earlier, can bolster states’ ability to exercise their sovereignty

[21] See Joint Chiefs of Staff, ‘Joint Publication 3-12 Cyberspace Operations’, 2 June 2018, https://fas.org/irp/doddir/dod/jp3_12.pdf.

in an operationally highly demanding milieu. Relevant actions include establishing international agreements as well as norms and regulatory frameworks for cyberspace. Examples of such arrangements are the United Kingdom's cybersecurity agreements with Singapore, India, NATO, Europol, and ASEAN. Second are "partnerships of access", which seek to secure access to computer nodes that a given state has identified as crucial to its national interest and against which it wishes to achieve some strategic or tactical effect. Such partnerships are constructed through state-level agreements and public-private partnerships. Third are "partnerships of knowledge" to gain situational awareness and initiative. Formal intelligence-sharing arrangements and joint research programmes foster such partnerships. Fourth are "partnerships to manoeuvre" that seek to enhance militaries' scope of tactical action. These partnerships can flow largely from existing ones – for example, the United Kingdom's joint operations with the United States and other nations against IS as well as the multinational and multi-agency operations to dismantle criminal networks (such as the 2016 Avalanche platform case).[22]

A second major point of discussion was NATO's role in fostering international cooperation and coordination. While NATO's collective defence clause against armed attack (Article 5) is often viewed as the Alliance's centrepiece, most of the organisation's activity in fact has occurred *below* the threshold of war – especially in the cyber defence context.

In the last three years, NATO has made significant progress in interallied cooperation. Nine allies have publicly volunteered to integrate "sovereign cyber effects" into NATO operations. From a tactical point of view, NATO has supported intelligence sharing by encouraging the birth of "communities of interest" and through the creation of a dedicated malware-sharing platform. From an operational standpoint, cooperation between allies has been enabled by joint exercises such as Cyber Coalition – NATO's flagship cyber defence exercise that tested the integration of sovereign cyber effects voluntarily as provided by allies. The Cyberspace Operations Centre at NATO Headquarters has responsibility for assisting such operationalisation of cyberspace as a domain.[23] Large exercises such as the 2018 Trident Juncture aimed to test allied interoperability as well as command and control. Finally, on a strategic and political level, NATO fosters collaboration via discussions in the Cyber Defence Committee and among Member State ambassadors.[24] In this regard, too, the recent Crisis Management Exercise featured a robust cyber scenario to educate officials at NATO Headquarters on the necessity for high-level cooperation.

C. Recommendations for Action or Further Enquiry

Trust problems among prospective or existing partners presents a major obstacle to successful partnerships. As such, governments should identify appropriate legal and policy frameworks that foster trust by setting ethical and moral standards to guide partner selection and conduct.

The discussion also recommended that before pursuing trust at the international level, it is important that governments solve cooperation problems within their *own* domestic setting –

---

[22] '"Avalanche" Network Dismantled in International Cyber Operation - Europol Press Release', EUROJUST, 1 December 2016, http://www.eurojust.europa.eu/press/PressReleases/Pages/2016/2016-12-01.aspx.
[23] Laura Brent, 'NATO's role in cyberspace', NATO Review Magazine, accessed 26 September 2019, http://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm.
[24] Brent.

particularly among public and private sector actors that often mistrust each other's motive and aims. These trust-building efforts would benefit from clear definitions of partnership success that help to clarify expectations and avoid misunderstanding.

Finally, the discussion highlighted states' tendency to extend their sovereignty to areas of cyberspace not their own. State practice is making it increasingly clear that sovereignty in cyberspace does not have the same meaning or expression as sovereignty in the physical space: states tend to be less restrained in extending their sovereign authority to cyberspace. Thus, interstate dialogue about how sovereignty is understood and applied in the cyber domain would aid the proper functioning of partnerships.

Concluding Remarks

Drawing from the input from leading thinkers and practitioners from various industries and nations, the workshop discussions allow us to draw important conclusions about the challenges and opportunities of transatlantic cooperation in the cyber domain.

One is the necessity to recognise, understand, and respect national differences in approaches to cyber strategy. Some nations – notably France – emphasise the necessity for robust sovereign action. Others – such as the Netherlands – express a special concern for consensus building and the preservation of international stability through the fostering of international norms of conduct. Still others –Estonia for example – stress the centrality of regional security cooperation within NATO. The national approaches are not wholly different; they may even be complementary; but they entail different kinds of policy emphasis.

Another important concern is the rapid pace of doctrinal development. How should we fit "campaign" thinking into cyber strategy – indeed, into the very meaning of cybersecurity? The discussions showed that such campaign thinking will require a Whole 0f Nation approach to security planning that requires states to draw from varied source of national power in both the public and private sectors. Another question is the difference – or similarity – between offence and defence. Can the distinction – essential in conventional military doctrine – survive in a domain in which the tactical necessities of protecting and disrupting computer infrastructure are often blurred? And where is the line between domestic and international activity in a terrain whose interconnections defy the neat definition of operational jurisdictions? This question in particular confronts the implementation of Defend Forward.

The benefits and obstacles of inter-allied cooperation also dominated much of the discussion. Special prominence was given to the expansion of Persistent Engagement, or the question of how operating in allied networks can affect trust among security partners. Partnerships in this domain matter, as discussants noted. But uncoordinated or unannounced operations within other partners' terrain may erode trust and the cohesion of relations. NATO here takes a crucial role: its seven decades of success fostering cooperation in conventional domains offers a strong basis on which to strengthen cyber ties among allies. The task requires changes in thinking – especially a notification framework to forewarn about friendly intrusions into allies' home networks.

Problems of cyber strategy and their manifestation in the transatlantic context are complex. The discussions highlighted significant progress in doctrinal thinking made in recent years.

Nevertheless, the practice of cyber defence continues to outpace thinking. Closing the gap of understanding requires further interallied and intersectoral discussion as fostered by this event.