CES Policy Brief [1]
June 2017

International Cyber Policy and Transatlantic Relations: Making States Responsible for Their Activities in Cyberspace

Dr. Annegret Bendiek[2] and Dr. Ben Wagner[3]
Stiftung Wissenschaft und Politik (SWP)

Cyberwar continues to be a hot topic in many of the discussions about the future of warfare. Yet despite the persistent debate about warfare on the Internet, it is questionable whether cyberwar has taken place in the past or is likely to take place in future. Ever since states engaged in international security policy have they been caught in the security dilemma. That dilemma has triggered arms races and repeatedly led to military confrontations. Since the Second World War, the international community has made significant progress towards taming the security dilemma by establishing arms control treaties, trust-building mechanisms, and a dense network of cooperation. The rise of offensive cyber operations today threatens to tear down those mechanisms and to introduce a renaissance of the security dilemma. The only way to prevent this from happening is to build norms and institutions that promote state responsibility and focus on "deterrence by resilience."

Without question, both civilian and military actors are engaged in a wide variety of offensive and defensive operations on the Internet. However, the scope and scale of such operations are

[1] This policy brief is part of a series funded by the Centre for European Studies Jean Monnet European Union Centre of Excellence (JMEUCE) and the Canada-Europe Transatlantic Dialogue (CETD) at Carleton University. The JMEUCE is funded in part by a grant from the European Union. CETD receives funding from the Social Sciences and Humanities Research Council of Canada (SSHRC). The contents of this publication are the sole responsibility of the author and in no way can be taken to reflect the views of the European Union, JMEUCE, CETD and SSHRC.

[2] Dr. Annegret Bendiek is a Senior Associate with the EU/Europe Research Division at the Stiftung Wissenschaft und Politik (SWP, German Institute for International and Security Affairs).

[3] Dr. Ben Wagner is an Associate with the Global Issues Research Division at the Stiftung Wissenschaft und Politik (SWP, German Institute for International and Security Affairs).

far more akin to espionage or covert operations and are considerably below the threshold of armed conflict, let alone warfare. Instead, "sabotage, espionage, and subversion" (Rid. 2012, p. 5) are more useful terms to understand the various forms of "cyber" operations.

Moreover, in debates about cyber conflict there are frequent assumptions that a wide variety of non-state actors are capable of engaging in extensive cyber conflict. While this may be technically feasible, the overwhelming majority of advanced offensive cyber operations is conducted by state actors or their direct proxies. Thus, debates about "cyber terrorism" bear little resemblance to the practical realities of everyday cyber attacks.

The interconnectedness of critical infrastructure, along with the growing "Internet of Things" (IoT), has compelled policymakers to consider how we defend, protect, and create resilient critical infrastructures. Whether these are attacks on critical infrastructure or attempts to steal critical information, digital technologies are so deeply enmeshed within all levels of modern society that it is difficult for society to function without them.

Deterrence by Resilience

Governments have begun to develop strategic postures on how to respond precisely because societies are so deeply interlinked with digital technologies. Within the existing debate there are two main approaches to respond strategically to such cyber threats: deterrence by resilience, and deterrence by retaliation (Bendiek and Metzger 2015). Deterrence by resilience involves strengthening key existing infrastructure and improving the overall *defensive* posture, making similar attacks far more difficult. On the other hand, deterrence by retaliation involves an *offensive* response to cyber-attacks to ensure there is no repetition, often without any prior knowledge about who the attacker is beforehand.

While reliable data on cyber operations is scarce, it is highly questionable whether deterrence by retaliation is an effective strategy for countering cyber threats. Lawrence Freedman (2004), one of leading academics on strategy and security policy, argues, "what we need to think about is not so much how to make deterrence work, but about what sorts of behavior we now wish to proscribe" (p. 118). Making such a strategy effective would require both a far higher level of attribution than is currently the case, as well as a willingness of states to constrain malicious attackers. Moreover, deterrence by retaliation comes with considerable legal and political risks, as it typically involves attacking unknown adversaries without *a priori* knowledge. At the same time, such offensive operations run the risk of degrading a common pool resource: trust in the stability and integrity of the Internet. By turning the Internet into a persistently escalating "cyberspace battleground," it becomes less reliable and trustworthy for everyone who uses it. Credible reports have suggested such offensive cyber operations carried out can go badly wrong as illustrated by the incident reported by Ackerman (2014) that U.S. cyber operatives may have accidently caused an extensive Internet outage in Syria in 2012.

In contrast, deterrence by resilience involves improving the defensive security of cyberspace, with a particular focus on critical infrastructure, which is perceived as the most vulnerable. This hardening posture involves none of the risks of offensive operations and comes with the added bonus of increasing the level of resilience against other forms of attacks such as cybercrime. However, there are persistent claims by security experts that resilience alone is insufficient to prevent cyber attacks. While some scholars would argue that you need a shield as well as a sword to defend yourself, others would recommend buying a better shield instead of a sword.

Within Europe, both the European Union and NATO have focused their strategies on deterrence by resilience, yet they emphasize different strategic areas. Some cyber powers, such as Great Britain, France, Germany, Sweden, the Netherlands, and Estonia, have started to enlarge their offensive and defensive cyber capabilities. Likewise, the EU and NATO have begun corralling their respective members to establish common defensive capabilities. Only a few countries within the EU and NATO, however, can deploy offensive capabilities so far. Many leading scholars have warned that the build-up of offensive capabilities only repeats the mistakes of the past, as it can foster mistrust, may provoke a new arms race, and might even lead to the Internet's disintegration as states increasingly assert their sovereignty.

Key Challenges of Cyber Operations

Beyond strategic posture, there are numerous challenges related to military cyber operations. While it is impossible to discuss all of them here, a few key challenges will be discussed in greater detail related to accountability, state-society attacks, and norms of behavior in cyberspace.

On the first point, offensive cyber operations frequently take place with little oversight and accountability. This is in part due to their unclear organizational structure, typically housed somewhere in between intelligence services of the military and private sector contractors. In part, these ad hoc institutional structures are a typical political response to acute political challenges. However, there is need for states to develop more sustained oversight and accountability mechanisms in order to ensure their legitimacy and longevity. The shift to separate U.S. Cyber Command from the National Security Agency (NSA) in order to "…draw cleaner lines between the government's military and intelligence cyber functions…" (Marks 2016) is a particularly interesting example. This starts a trend for a stronger split between military and so-called loud cyber weapons on the one hand and intelligence cyber operations on the other.

The second point, usage of cyber attacks as a tool of state repression, has received insufficient attention thus far in debates about cyber security and cyber war. States engaging in cyber attacks against their citizens have become increasingly common in the past decade, with steadily escalating forms of attacks. The Syrian government's shutdown of mobile phone networks in close coordination with military operations (Gohdes 2015), the Tunisian government actively stealing the data of all Gmail users based in Tunisia around the Tunisian uprisings (Wagner 2012) and the government of Pakistan shutting down all mobile phone and Internet connections on a regular basis in the country (Purdon, Ashraf, and Wagner 2015) are examples of state attacks. While it is common in the literature to discuss a potential cyber attack on critical infrastructure by third parties—such as the purported shutdown of the North Korean Internet by U.S. government operatives in 2014—it is often the case that many states are equally eager to attack their own critical communications infrastructure. Cyber attacks by states against their own critical communications infrastructure serve to degrade the quality of existing societal infrastructure and harm economic development. These attacks typically occur around elections and mass protests, and are swiftly becoming a global phenomenon.

Finally, Freedman is right to point to norms as the main objective now. He writes that "the wider objective therefore has to be to encourage the development of an international order in which there are formidable restraints on the use of force" (p. 119). Policymakers' and cyber diplomacy attention has been focused on finding agreement on common norms for state behavior in cyberspace, with mixed success (Bendiek 2016). In 2000, the United Nations

General Assembly called on states "to ensure that their laws and practices eliminate safe havens for those who criminally misuse information technologies" (p. 2). The UN Group of Governmental Experts (UN GGE) picked up this idea in its final report of June 2015. According to the report, all states shall ensure that their territories, and especially the computer systems and infrastructure situated there or otherwise under the states' control, are not misused for attacks on the infrastructure of other states. This emphasizes an approach which hardens existing infrastructure and mitigates the risks that stem from existing infrastructure. This has led the GGE to recommend in its report, "States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions" (p. 8). This is important because each individual vulnerability, cyber-attack, and weakness in defensive capacity can lead to individual users losing control of their devices and the possible weakening the Internet as a whole. Therefore, ensuring the stability and integrity of the Internet is a crucial goal for policymakers, and, in the words of the GGE, a "*key question for international peace and security*."

References:

Ackerman, Spencer. (2014). "Snowden: NSA Accidentally Caused Syria's Internet Blackout in 2012," *The Guardian*, August 13, 2014. https://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war .

Bendiek, Annegret. (2016). "Due Diligence in Cyberspace: Guidelines for International and European Cyber Policy and Cybersecurity Policy," *SWP Research Paper 7*, May 2016, SWP, Berlin. https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf

Bendiek, Annegret and Tobias Metzger. (2015). "Deterrence Theory in the Cyber-Century: Lessons from a State-of-the-Art Literature Review," *SWP Working Papers*, May 2015, SWP, Berlin. https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf

Freedman, Lawrence. (2004). *Deterrence*. Cambridge: Polity Press.

Gohdes, Anita R. (2015). "Pulling the Plug: Network Disruptions and Violence in Civil Conflict," *Journal of Peace Research* 52(3): 352-367. http://jpr.sagepub.com/cgi/doi/10.1177/0022343314551398 .

Marks, Joseph. (2016). "The NSA-Cyber Command Divorce Is Inching Closer to Reality," *Defense One*. December 1, 2016. http://www.defenseone.com/politics/2016/12/nsa-cyber-command-divorce-inching-closer-reality/133559/ .

Purdon, Lucy, Arsalan Ashraf, and Ben Wagner. (2015). "Security vs. Access: The Impact of Mobile Network Shutdowns," *Digital Dangers Case Study Number 3*, September 2015 (London: Institute for Human Rights and Business). https://www.ihrb.org/uploads/reports/2015-09%2C_IHRB_Report%2C_Security_v_Access_-_The_Impact_of_Mobile_Network_Shutdowns.pdf

Rid, Thomas. (2012). "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35(1): 5-32. http://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939

United Nations General Assembly. (2001, 22 January). "Resolution 55/63: Combating the Criminal Misuse of Information Technologies." https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

United Nations General Assembly. (2015, 22 July). “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” http://undocs.org/A/70/174

Wagner, Ben. (2012). “After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy,” Briefing Paper, July 2012 (Brussels, Belgium: European Union). http://www.europarl.europa.eu/RegData/etudes/note/join/2012/457102/EXPO-DROI_NT%282012%29457102_EN.pdf