March 2020

KONRAD ADENAUER STIFTUNG

Active Cyber Defense- A comparative study on US, Israeli and German approaches

What is Active Cyber Defense?

Dr. Sven Herpig, Robert Morgus, Dr. Amit Sheniak

Active Cyber Defense is an actively deployed countermeasure which is considered below the threshold of armed conflict, with the goal of defending against, or attribute a cyber operation. The following section breaks potential countermeasures into the following categories:

1.Defense with a Twist
2.Hacking Back
3.Persistent Engagement and Defending Forward

Although official government publications provide a few general definitions, the categories mentioned above stress that "active cyber defense" tends to be associated with two main policy issues. First, as part of a deterrence by punishment strategy which is aimed at improving a state's national security. Secondly as a technical and operational defense system. This includes an attribution mechanism which is implemented by state agencies often with support of private entities. While there is occasionally overlap, the dichotomy between strategic and operational levels, as well as the public and private sector roles, is crucial to understand the challenges states face. It is one of the main obstacles for decision-makers preventing the implementation of coherent policy responses.

1. Defense with a Twist

There are several tools used to bolster defense capabilities that can improve the security and resilience of both IT systems and networks. A common example would be antivirus software, which is tasked with detecting malicious software or firewalls which should separate legitimate from illegitimate access and block the latter. For those and many more tools their use as strictly defensive instruments is straight forward. However, there are IT security tools and mechanisms which can be used actively and invasive manner. They are therefore frequently mentioned during the active cyber defense debate. They include honeypots, canary tokens, sinkholing, walled garden, traffic redirection, forensics on server snapshots amongst others.

The example of canary tokens might illustrate the role that a specific subset of security mechanisms can play in active cyber defense. A canary token can come in a variety of different shapes and forms but is basically a software addendum - e. g. to an existing file like a document or a user account – that that can trigger a predefined

action. It can for example sound an alarm once it is copied from a certain directory or network. The information provided by the token could help to better track and identify the attacker. More invasive variants of this software could even try to trigger a data wipe on the adversary's system where it was copied to. Thus, it is a security mechanism that helps to protect data, enable security agencies to track it when it's illegitimately copied or even cause damage to external IT systems. Therefore, it is not a straight-up passive-defensive security tool.

2. Hacking Back

Among the different actions that characterized active cyber defense, is the use of offensive capabilities, known as "Hack-Backs," to retaliate against an attacker. This is defined by the United States Congress as: "any measure undertaken by… a defender and consisting of accessing without authorization the computer of the attacker to the defender's own network to gather information in order to establish attribution of criminal activity… disrupt continued unauthorized activity against the defender's own network; or monitor the behavior of an attacker to assist in developing future intrusion prevention…".[1]

Hack-Backs is a symptom of the challenges posed by the existing inability of (western) national cybersecurity entities to provide sufficient defense to the private sector. This is exacerbated by national governments unwillingness to implement policies that succeed in cultivating a sense of deterrence against potential attackers.[2] Hack-Backs have magnified a decade-long policy dilemma for states: should states act to legalize offensive cyber countermeasures or potentially "privatize" offensive cyber-actions taken by private entities, in order to possibly enhance security? Or should states prevent such steps so as to avoid the possible unintended mistakes? [3] Additionally, states must take into consideration the need to prevent the gradual erosion of state's sovereignty due to cybersecurity. The fact that some states are considering various legal tools to formalize Hack-Backs, serves as acknowledgment of the state's inability to confront these challenges in effective ways. While most national cybersecurity policies today tend to concentrate on the inter-state cyber relations while ignoring the growing economic costs to the private sector due to cyber-attacks.

3. Persistent Engagement & Defending Forward

Persistent engagement is the concept that states must "persistently contest malicious cyberspace actors" in order to increase resiliency.[4] Persistent engagement is a response to the observation that "cyberspace is a fluid environment of constant contact and shifting terrain," and that "new vulnerabilities and opportunities continually arise as new terrain emerges."[5] According to the United States Department of Defense, "cyberspace's structural feature of interconnectedness and its core condition of constant contact creates a strategic necessity to operate continuously in cyberspace."[6]

To effectively engage persistently, states must "defend forward as close as possible to the origin of adversary activity."[7] A strategic response to the observations around constant contact and persistent engagement, defend forward is the name for a set of activity that falls under the strategy of the United States Cyber Command, wherein

[1] https://www.congress.gov/bill/115th-congress/house-bill/4036/text
[2] https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back
[3] https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act
[4] https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, p. 4
[5] https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, p. 4
[6] https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace
[7] https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, p. 4

a defender uses intelligence to identify a threat and takes steps to disable that threat's capability at its source. The goal of defending forward is to "disrupt… adversaries' freedom of action."[8]

Defending forward and persistent engagement can serve two purposes. First, as demonstrated by the U.S. operation against the Russian Internet Research Agency (IRA), defending forward can be a means to blunt an adversary's capability that may be used or is being used against a defender. In these cases, defending forward has been likened to kicking the knife out of the hand of an attacker.[9] However, defending forward and persistent engagement can also serve the function of deterring adversarial activity by demonstrating that the defender holds certain adversarial assets at risk. Persistent engagement and defend forward are not without risks, however. As Healey notes, it can be difficult for an adversary to decipher intent and therefore can spark escalation.

Three Approaches: Germany, Israel, and the U.S.

Germany

To better understand Germany's approach towards security and national defense, it helps to focus on its geographic position in the heart of Europe during the longest period of peace on the continent. Politically, experiences drawn from the two World Wars and the repressive East German regime have led to strong anti-military and anti-surveillance postures with a focus on data security and privacy. Germany has both a highly active academia and civil society which includes the famous hacker collective 'Chaos Computer Club,' amongst other similar organizations.[10] This community is very vocal on issues such as privacy infringements, government surveillance powers, and the offensive use of cyber capabilities. They are known for even bringing these cases to the country's highest court for litigation. [11]

For the longest time, Germany has been on a path to promoting cybersecurity through IT security and resilience measures rooted almost entirely in the civilian domain. Even though Germany has yet to entirely deviate from this approach, recent events increasingly point towards significant change triggered by the moderately successful cyber operation against the German Federal Parliament in 2015.

In 1991, Germany unveiled its new approach towards IT security when it decoupled its security and encryption experts from the intelligence sector, creating a new national cyber security agency under the supervision of the Ministry of the Interior. [12] In terms of staff and responsibilities, this newly created national cyber security agency (*Bundesamt für Sicherheit in der Informationstechnik*), grew to 950 personnel and a annual budget of 118 million Euros by 2018.[13] The agency is responsible for protecting government networks, cooperating with the private sector and supporting society's efforts to battle cybercrime.[14]

[8] https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010, p. 4
[9] https://www.thecipherbrief.com/column/cyber-initiator/taking-down-russian-trolls-is-my-kind-of-cyber-attack
[10] https://www.ccc.de/
[11] https://www.golem.de/news/verfassungsbeschwerde-digitalcourage-klagt-gegen-staatstrojaner-1808-135878.html
[12] https://www.stiftung-nv.de/sites/default/files/cybersicherheitspolitik_in_deutschland.pdf
[13] https://www.bsi.bund.de/DE/Presse/BSI-Kurzprofil/kurzprofil_node.html
[14] https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

Germany: a security defensive-focused approach

Through 2015, Germany enacted a number of prominent policies, strategies and regulations. to enhance the country's cybersecurity. This included the 'Crypto Principles' (1999)[15], 'The National Plan Information Infrastructure Protection' (2005)[16], its first 'National Cyber-Security Strategy' (2011)[17], the 'Digital Agenda' (2014-2017)[18] and the IT Security Act (2015)[19]. These various protocols were defensive in nature, focusing on increasing Germany's IT security and resilience, leading to the creation and coordination of federal agencies to enhance cybersecurity[20]. Germany's cybersecurity strategy 2011 is defensive in nature, with no explicit mention of offensive cyber operations; cooperation with NATO is narrowed to mutual agreement of cyber security protocols. Yet, cooperation with NATO on in the cyber security realm may in future lead to an increased offensive posture including active cyber defense. The need for a holistic set of tools to defend against cyber-attacks, based on a constant monitoring of the overall security situation is paramount for effective cyber defense protocols.

Attack on the parliament: a turning point but no shift towards defending forward or persistent engagement

The turning point in Germany's strategic posture is likely the allegedly Russian-backed cyber operation against the German Parliament.[21] The data, which was copied by the attackers, was not overly sensitive and the attack was not sustained over a long period of time before Germany's agencies were able to stop it. However, it created a formidable narrative for German military, intelligence and security agencies, in which they demanded increased powers and tools within the cyber domain.

As response to the breach of the parliament's network, the government issued an updated cybersecurity strategy in 2016. This includes specific references to the use of offensive cyber capabilities, cyber defense and deterrence.[22] In the following years, Germany consolidated its military personnel working on IT security and cyber defense into one unified command (*Kommando Cyber- und Informationsraum*), created a centralized public provider for acquiring vulnerabilities, hacking tools and services as well as big data analysis (*Zentrale Stelle für Informationstechnik im Sicherheitsbereich*) and announced the foundation of a joint civil-military DARPA-like agency to foster cybersecurity and cyber defense research (*Cyber-Agentur*).

Hackbacks as middle ground?

Since the federal parliament's network has been compromised, the Germany military, intelligence and security agencies have been pushing for a political and legal framework that allows for active cyber defense measures thereby admitting that there was no legal or strategic basis for active cyber defense measures.[23] The 2019 provisions were meant to alter this state of affairs with three legal packages: updated IT security legislation, the synchronization of domestic intelligence legislation and undisclosed computer network interference

[15] https://www.lawfareblog.com/germanys-crypto-past-and-hacking-future
[16] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/cs_Strategie_node.html
[17] https://webcache.googleusercontent.com/search?q=cache:Bec_Kjgcp4EJ:https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf%3F__blob%3DpublicationFile+&cd=1&hl=de&ct=clnk&gl=de
[18] https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda.pdf?__blob=publicationFile&v=3
[19] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1562915497762
[20] https://www.stiftung-nv.de/sites/default/files/cybersicherheitspolitik_in_deutschland.pdf
[21] https://www.stiftung-nv.de/sites/default/files/tcf-defending_political_lt-infrastructures-problem_analysis.pdf
[22] https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf
[23] https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them

amendments.[24] The first two packages were supposed to be passed by June 30, 2019 but have yet to be taken to the parliament floor for voting procedure due to criticism from the cybersecurity experts community[25], parliamentarians[26] and the Ministry of Justice and for Consumer Protection[27].

Regardless of the legislation that will legally permit active cyber defense in future, it will continue to be a hotly debated topic within the German cybersecurity policy sphere. If respective laws are passed, they will likely face legal challenges within the Constitutional Court (*Bundesverfassungsgericht)*. This should not be surprising as Germany has a history of focusing on IT security and resilience rather than offensive cyber operations. It is not unlike the Germany government's stance on data protection with widespread support from the German public. The fact that past cyber operations such as WannaCry or the intrusions of the German parliament and the Federal Foreign Office (*Auswärtiges Amt*) did not lead to severe damages can be regarded in support of Germany's purely defensive stance. Lastly, Germany's foreign policy is focused on norms building, maintaining stability in cyberspace and capacity building for increased resilience and IT security.

Germany's experience and value-driven approach towards increasing cybersecurity through IT security and resilience rather than offensive cyber operations has yet to be proven wrong. The recent attempt at a more offensive posture through legislation on "defense with a twist" and "hacking back" capabilities may come with unintended consequences. In a setting with limited resources, every hour spent on the offensive is an hour less spent on the defensive, and the current German active cyber defense approach increasingly seems offensive in nature.

Israel

It seems that in Israel, national cyber security policymakers have acknowledged the centrality of the Israeli hi-tech innovation ecosystem, as a key factor of the county's posture in the cyber domain. Thus, the independence and strength of the cyber private sector, is perceived as the one of the main pillars in the ability of the state to provide security. Therefore, the state has adopted a notion that the government should allow some form of self-regulation and avoid the prevention of cyber-services including some private active-defense measurements. Another important factor that has contributed to a favorable opinion towards cyber-active-defense, is Israel's national security doctrine, which emphasize the need to promote defense by active and sometimes offensive actions beneath the threshold of armed conflict.

The Cyber-Law Environment in Israel: A broad space for legal discretion?

In 1981, Israel enacted the Protection of Privacy Law (5741), commonly referred to as the "Privacy Law". This created minimum security standards of privacy protection of personal data within the state. In 1996 this law was amended to adapt to technological advances, and was accompanied by the passage of the Patients' Rights Law (5756), which also covered the protection of personal data. In 2013, Israel became a signatory to the Budapest Convention on Cybercrime (CETS 185), and has enacted a law forbidding illegal access to computers and other computer-related crimes in 1996 and has joined the Council of Europe Convention on Cybercrime (COE 185). As of today, Israeli law, therefore, forbids an actor to access/act on another organization's network without consent". Government agencies obviously have a legal basis to carry out their activities.

[24] https://netzpolitik.org/2019/aktive-cyber-abwehr-innenminister-schaltet-bei-it-sicherheit-schrittweise-von-verteidigung-auf-angriff/
[25] https://www.bundestag.de/dokumente/textarchiv/2019/kw15-pa-inneres-630106
[26] https://wirtschaft.com/it-sicherheitsgesetz-union-hofft-auf-ende-der-spd-blockade/
[27] https://www.waz.de/politik/justizministerium-bremst-plaene-zur-ueberwachung-von-kindern-id216757081.html

In 2015, the Israeli Supreme Court interpreted this clause broadly,[28] enabling the State Attorney in Israel, which is the head of the criminal prosecution, to develop prosecutorial guidelines as to cases which will be indicted. At present, the distinction between the legality of different activities which include "access" to another computer network, lies with the State Attorney. As a general observation, it appears that cases where access involves "overcoming of a technological lock" that otherwise protects access, would be deemed as "severe" breaching, and stress the illegality of an access to a computer's data without consent.[29] The broad discretion of Israel state attorney to interpret the law, provides the state with the ability to allow different forms of cyber-active-defense actions, by creating a defined legal "gray-area" for private entities to defend themselves and for cyber-active-defense services to exist.

The Israeli Cybersecurity Private Sector as the Axis of Israel's Cyber Strategy

In 2015, Israel adopted a national strategy to mitigate attacks that break organizational defenses. A major element of this strategy was to enhance coordination of various organizations, by cultivating and enhancing the thriving cybersecurity innovation ecosystem. The centerpiece of the strategy was the establishment of the new Israeli National Cyber Directorate (INCD) formulated in a series of government resolutions between 2011 to 2017,[30] whose main aim was to monitor and defend the private sector and incentivize its advancement in innovation and workforce. This, alongside its responsibility for the security of Israel's critical infrastructures, the INCD was nominated as the official interlocker between the government and private sector. Working under the guidelines of government decision no. 2443 of 2015, to advance the defense of the private sector by promoting private cybersecurity services, this might include cyber-active-defense services. [31] This mission was also evident in the national operational cybersecurity strategy of 2015. The strategy is based on a three-layer framework, of which the first layer aims for coherent effective implementation of appropriate cybersecurity defenses by the private sector itself.[32]

Some of the Israeli companies who provide cyber services proved to be a challenge to the a Israeli authorities due to the use of offensive means which drew international criticism (i.e. Israel's NSO group).[33] But these challenges were balanced by the gains to Israeli security entities who later benefited from incorporating the knowledge, innovations and methodologies developed by the private sector, to be able to provide security and project force. The private and the public cybersecurity sectors are part of the same ecosystem, in which most young Israeli cyber experts start by serving in the IDF cyber unites (under a mandatory conscription law), and later utilize their military knowledge and experience in the private sector, bring new knowledge and insights from the private sector back to the IDF during their annual military reserve service or as part of a combined official and private sector projects.

---

[28] See The State of Israel Vs. Ezra of December 15th, 2015. https://www.law.co.il/computer-law/2015/12/15/israel-v-ezra-supreme-court-appeal/ [in Hebrew]

[29] See Israel State Attorney's guidance No. 2.38 of August 27th, 2018. https://www.justice.gov.il/Units/StateAttorney/Guidelines/02.38.pdf [in Hebrew].

[30]https://www.gov.il/en/departments/about/newab

[31]See resolution 2443 of the 33rd Israeli Government, February 12th, 2015, Sec. 1. [in Hebrew] https://www.gov.il/he/Departments/policies/2015_des2443

[32]Dr. Eviatar Matania the founder and former head of the INCD, described the "three layer model" in an academic article published at 2016. see Matania, E., Yoffe, L., & Mashkautsan, M. (2016). "A Three-Layer Framework for a Comprehensive National Cyber-security Strategy". *Geo. J. Int'l Aff.*, 17, 77.

[33]https://www.reuters.com/article/us-socialmedia-un-spyware/u-n-surveillance-expert-urges-global-moratorium-on-sale-of-spyware-idUSKCN1TJ2DV

"Active-Defense" as a main characterization of Israeli security cultural

On May 5th, 2019 during a day of skirmishes on the border of the Gaza Strip between the Palestinian militant organization Hamas and Israel, the IDF spokesman disseminated the following massage over twitter: "Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed".[34] The attack drew international attention and was perceived by some as a new and dangerous precedent in cyber-active-defense, due to its cross-domain nature, some observers even questioned the legality of the attack it-self. Although this attack might seem as an extreme active-cyber-defense tactic and a new cyber-deterrence strategy, it does not fall clearly under our definition of Cyber-Active-Defense. Instead one should analyze the attack as an expression of the general Israeli security culture, which had an effect on the offensive Israeli cyber-deterrence strategy.

Israel's bitter experience in the military operations it launched in Lebanon, the West Bank, and the Gaza Strip has led to a gradual shift away from "decisive," large-scale military operations to "fighting in rounds." This shift is based on the premise that conflicts can be postponed by military action short of a direct confrontation. Hence, the IDF has adopted the notion of "Campaign Between Campaigns" (CBC):[35] an ongoing campaign that constantly seeks to challenge potential adversaries, decreasing their ability to inflict harm upon Israel in the next "round".[36] The escalatory nature of conflict on May 5th 2019 can be seen as another action in the chain of CMC attacks that are part of Israel's ongoing de-facto security doctrine.

The shift of the Israeli security doctrine to CBC, overlapped with the advancement of the cyber realm to become a further dimension of force employment. The de-territorial nature of cyber-attacks and the technological constraints that states face when trying to attribute such actions to a specific attacker and the lack of defined international norms, made cyber-attacks suitable for low intensive conflicts (LICs) beneath the threshold of armed conflict. Indeed, the IDF acknowledged its use of cyber operations in "thwarting initiatives by Israel's enemies to undermine the IDF's and Israel's operational freedom in a wide variety of conflicts,"[37]thus describing it as part of CBC. In 2009, the IDF established a dedicated cyber headquarters subordinate to the office of the IDF's deputy chief of staff,[38]which later (in 2015) became a Cyber Defense Division under the army's C4I and Cyber Defense Directorate.[39] At the same time, operational and intelligence cyber capabilities remain the responsibility of Israel's SIGINT National Unit (ISNU or Unit 8200) in the Israeli Defense Intelligence (IDI).[40] The institutionalization of cyber military operation under the Intelligence and special operation sections of the IDF, serve as another evidence for the adaptation of cyber-active-defense as another tool in the CBC doctrine, and not as part of a normative change regarding cyber-attacks. In a way, this cyber-strategy can be described as an Israeli version of the U.S Persistent Engagement strategy.

[34]https://twitter.com/idf/status/1125066395010699264?lang=he

[35]In Hebrew: *Ha-ma'aracha she-bein ha-ma'arachot*(MABAM).

[36]Shai Shabtai, "The Doctrine of Campaign between Campaigns," *Ma'arachot*, 445 (2012), 24 [Hebrew].

[37]Yaacov Katz, "IDF Admits to Using Cyber Space to Attack Enemies," *Jerusalem Post*, March 6, 2012, available at: https://www.jpost.com/Defense/IDF-admits-to-using-cyber-space-to-attack-enemies(Accessed: February 19, 2019).

[38]Nati Cohen "The 5th Domain: IDF Preparation for a Vast Cyber-attack," *Ma'arachot*, 452 (2013): 13 [Hebrew].

[39]See the website of the C4I and Cyber Defense Directorate, https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate (Accessed: February 19, 2019).

[40]Lior Tabansky and Isaac Ben-Israel, *Cybersecurity in Israel* (New York: Springer, 2015), 64.

United States

The United States is currently reexamining its approach to national cybersecurity. Although the persistent engagement and defend forward strategy documents are products of the Department of Defense, the strategy does incorporate other aspects of the U.S. government, most notably law enforcement entities. While the popular refrain in the U.S. is that cyber defense is "not working", a reasonable argument can be made that the U.S. has not really tried to construct a comprehensive cyber defensive strategy.

Cyber Defense

The primary department tasked with the policy and operations of cyber defense is the Department of Homeland Security (DHS), though the departments of Commerce, Defense, Energy, Treasury, and Justice all play roles as well. Within DHS, the Cybersecurity and Infrastructure Security Agency (CISA) houses both cyber policy and operational capacity and recently released its strategic plan for building cyber defensive capacity and resilience in the private sector.

While the specifics of "defense with a twist" as described in this report are not front and center in the strategy, many of the activities encompassed by defense with a twist are allowed under U.S. law and often encouraged as part of good practices in cyber defense. However, given the restrictions of the Computer Fraud and Abuse Act, which criminalizes unauthorized access to computer systems, uncertainty persists in the private sector regarding the legality of any activity that goes outside of an owned network. The blurred line between activities like honey potting and actively hacking into attacker networks has led some in the private sector to refrain using more active defense measures within their own systems.

Hacking Back

The Computer Fraud and Abuse Act of 1984 (CFAA) criminalizes accessing a computer or computer system without authorization or in excess of one's authorization.[41] The CFAA effectively outlaws the practice of hacking back for the private sector. However, over the course of the last five years, the US legislature has entertained loosening these restrictions to enable the private sector to conduct hacking back operations to better defend themselves in cyberspace. Congress' deliberation over hacking back, which has largely mirrored public conversation in the US, manifest in the Active Cyber Defense Certainty Act (ACDC).[42]

The ACDC was initially proposed in 2017 and gained little traction. The bill was proposed again in June 2019 with several updates, which included clearer notification requirements for companies intending to hack back and more specificity regarding the types of activities allowed under the proposed bill, creating, for example clearer legal exemptions for companies gathering data for the purposes of attributing cyber-attacks.[43] The proposal's reception in the American private sector was mixed, with some companies coming out strongly in favor and others insisting that the authorities to hack back should remain with the government only.[44]

Persistent Engagement & Defending Forward

Persistent engagement and defending forward are terms coined by U.S. Cyber Command and are integral parts of the U.S. Department of Defense's cybersecurity strategy. The primary debate within the U.S. cyber policy community regarding defending forward and persistent engagement now revolves around the question of where

[41] https://www.law.cornell.edu/uscode/text/18/1030
[42] https://www.congress.gov/bill/115th-congress/house-bill/4036
[43] https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act
[44] https://www.scmagazine.com/home/security-news/cybercrime/hacking-back/

U.S. government entities should be authorized to engage adversaries, re-popularizing the concepts of blue, grey, and red spaces.

Blue space refers to networks and devices owned and/or protected by the defender. Red space refers to networks and devices controlled—to the exclusion of others—by the adversary or attacker. Grey space refers to the rest of cyberspace. Grey space can be leveraged by an attacker to, for example, route an attack or magnify a distributed denial of service (DDoS) attack.

In an article for Joint Force Quarterly, National Security Agency and Cyber Command Director General Paul Nakasone notes that, "if we are only operating in 'blue space,' we have failed."[45] Nakasone's words suggest that the U.S. Cyber Command interprets its authorities to include operating in red space and possibly grey space. As Max Smeets observes, this could include operating in "routers in Nairobi, servers in Denmark or operating infrastructure in any other country around the world." [46]

To date, the two most prominent and publicized manifestations of Cyber Command's defend forward and persistent engagement strategies both involve engaging Russian actors. First, in November 2018, around the midterm election in the U.S., a Cyber Command unit conducted an operation that purportedly prevented the Internet Research Agency from spreading election-related mis- and disinformation. Jason Healey described this operation as one designed to "stop adversaries from punching you," but that it was not about deterrence or signaling.[47] Others have suggested that it serves both the purpose of stopping an ongoing attack and signaling to an adversary.[48]

The second notable manifestation of the strategy was unearthed in June 2019, when John Bolton, then the lead White House national security advisor, told media that the U.S. would target adversary systems "to say to Russia, or anybody else that's engaged in cyber operations against us, 'You will pay a price.'" According to David Sanger, these targets include things like power grid infrastructure.[49] The authority for Cyber Command to conduct such operations was granted by both the White House and Congress in the National Defense Authorization Act for 2019.[50]

Conclusion and Outlook

It is clear that Germany, Israel and the United States have different approaches to active defense in the cyber domain. While slowly moving toward offense, Germany has favored a purely defensive approach which does not allow government agencies to hack back. Israel has taken a different approach, in which it is not shy when it comes to hacking back. Similarly, the United States, is exploring options for enabling and legitimizing private sector actors to conduct hack back operations. The American approach is most transparent in its willingness to conduct what many in the United States would consider offensive operations in pursuit of greater security. Its behavior might even be regarded as proactive cyber defense as it relies on having a constant foothold in strategically relevant networks and IT systems.

---

[45] https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1736950/a-cyber-force-for-persistent-operations/
[46] https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies
[47] https://www.thecipherbrief.com/column/cyber-initiator/taking-down-russian-trolls-is-my-kind-of-cyber-attack
[48] https://www.washingtonpost.com/opinions/the-us-military-is-quietly-launching-efforts-to-deter-russian-meddling/2019/02/07/4de5c5fa-2b19-11e9-b2fc-721718903bfc_story.html?noredirect=on&utm_term=.42504703a905
[49] https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html
[50] https://www.congress.gov/bill/115th-congress/house-bill/5515/text

At this point all three approaches are seemingly a reflection of national security doctrines and defense cultures as well as the countries' respective roles in geopolitics. As the cyber domain differs from other domains, there are a number of open questions that need to be answered before we can answer the question which approach towards active cyber defense protects national interests the best, and indeed different approaches may work better for different countries. Nonetheless, the first question that comes to mind is whether security and resilience measures have failed and that is why states such as the United States and Israel are moving towards a more offensive stance in cyberspace or whether states and the private sector have simply not tried hard enough to invest resources and implement the measures to make life difficult for the attackers. If the assumption is that states need active defense to increase their own security, then they need to evaluate whether it should be limited to government entities or should be extended to the private sector as well. Aspects such as accountability, conflict escalation, arms control and norms, and ultimately a cost-benefit rationale are essential to this debate. In both cases, public and private sector active defense, the issue of oversight is crucial and is closely connected to issues surrounding attribution and conflict escalation. Especially in cases such as persistent engagement, where the use of cyber capabilities takes place before the adversary actually attacks. Moving to the international level, active defense needs to be evaluated on the basis of whether it can be counted as self-defense and under what conditions, or not. Likewise, what options do states have which infrastructure is a casualty of the "grey zone" of two adversaries, yet itself is not actively participating in that conflict.