Rethinking European Cyber Defense Policy: Toward a Defense Superiority Doctrine

Weber, Valentin

Veröffentlichungsversion / Published Version
Stellungnahme / comment

Empfohlene Zitierung / Suggested Citation:
Weber, V. (2022). *Rethinking European Cyber Defense Policy: Toward a Defense Superiority Doctrine.* (DGAP Policy Brief, 8). Berlin: Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V.. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-80023-9

No. 8
April 2022

DGAP POLICY BRIEF

Rethinking European Cyber Defense Policy

Toward a Defense Superiority Doctrine

Valentin Weber
Research Fellow,
Technology and Global
Affairs Program

The United States has abandoned old-fashioned thinking that focused on deterring cyber operations below the threshold of armed conflict. It now opts for a new doctrine of "persistent engagement" in cyberspace, which emphasizes offensive cyber operations to shape the behavior of adversaries. Rather than follow in the footsteps of the US, the EU should shape cyberspace into an environment of defense superiority, thereby helping forestall attacks both at *and* below the level of armed conflict.

– **The European Union should implement systemic measures to improve cybersecurity by encouraging encryption and redundancy in critical systems, as well as increasing the speed of patching and the quality of open-source software.**

– **The EU needs to engage in strategic capacity-building abroad, setting geographical priorities in Southeastern Europe and the Middle East, as well as South and Southeastern Asia.**

– **It must foster the deception of attackers through decoy network elements.**

– **EU member states should envisage conducting limited cyber operations to disrupt ongoing attacks.**

The European Union lacks a doctrine in cyberspace, concluded Thierry Breton, EU Commissioner for Internal Market, in 2021.[1] The EU's current cyber strategy from December 2020 neglects to develop such a doctrine; instead, it engages in traditional deterrence thinking, which aims to deter attacks through denial and punishment.[2] This strategy ignores the fact that measures of denial and punishment have been largely unsuccessful in deterring malicious international behavior below the threshold of armed conflict. While the EU's focus on the gradual increasing of resilience and reducing the incentive for attack through sanctions and verbal condemnations is necessary, it is insufficient for fending off cyber operations.[3] In December 2021, a cyber operation targeting the Belgian Ministry of Defense compelled segments of its network – e.g., its mail system – to be taken offline for days.[4] In January 2022, Germany's domestic intelligence service, the Bundesamt für Verfassungsschutz, revealed that APT27, a Chinese hacking group, had been stealing intellectual property from German pharmaceutical and technology companies.[5] Both of these incidents show that adversaries are not deterred from conducting operations despite potential punitive measures.

For its part, the United States has recognized that old deterrence thinking needs updating and has consequently changed its own doctrine and strategy for cyberspace. The current US strategy of *defending forward* emerges from a doctrine that considers traditional deterrence thinking as not appropriate for fending off attacks below the threshold of armed conflict. In other words, despite attempts to focus on denial and punishment, the United States continued to be hit by attacks such as the Sony Pictures hack and Office of Personal Management hack. The new US strategy of defending forward also emerges from the doctrine of *persistent engagement*. Persistent engagement rests on the belief that states like China, Russia, Iran, and North Korea engage in *persistent opportunism* in cyberspace and need to be countered constantly, rather than only in the event of a major attack.[6] The idea is to change the behavior of the adversary by engaging them globally, close to the source of malicious behavior. This means breaking into foreign systems, sometimes on allied territory.[7] Resilience and defense are also part of the US posture, but they are mentioned only marginally.[8]

EU member states have mostly restrained themselves from taking an overtly offensive cyber posture or using their offensive capabilities because they fear further propelling the digital arms race. The experience of the United States confirms these fears since the bold US narrative is likely to incite the further militarization of cyberspace.[9] If all countries, including China, engaged in this kind of offensive thinking,

EU CYBERSECURITY STRATEGY

On December 16, 2020, the EU presented its new strategy for cybersecurity. On the one hand, this strategy attempts to achieve denial through regulation of the EU market, which promotes resilience of devices, networks, and actors on EU territory. On the other, it attempts to do so through capacity-building abroad. Punishment may be applied if a hostile state disregards norms of responsible state behavior by, for example, attacking national critical infrastructure or undermining democratic processes. In this case, the EU strategy recommends the use of the EU Cyber Diplomacy Toolbox.

1 Thierry Breton, "How a European Cyber Resilience Act Will Help Protect Europe," European Commission, September 16, 2021: https://ec.europa.eu/commission/commissioners/2019-2024/breton/blog/how-european-cyber-resilience-act-will-help-protect-europe_en (accessed March 29, 2022).

2 European Commission, "New EU Cybersecurity Strategy," December 16, 2020: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 (accessed March 29, 2022).

3 European Commission, "New EU Cybersecurity Strategy," December 16, 2020: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 (accessed March 29, 2022)

4 *The Brussels Times*, "Belgian Defence Ministry Network Partially Down Following Cyber Attack," December 20, 2021: https://www.brusselstimes.com/belgium/198521/belgian-defence-ministry-network-partially-down-following-cyber-attack (accessed March 29, 2022).

5 Reuters, "Chinese Hackers Target German Pharma and Tech Firms," January 27, 2022: https://www.reuters.com/world/chinese-hackers-target-german-pharma-tech-firms-2022-01-26/ (accessed March 29, 2022).

6 Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *The Cyber Defense Review*, 2019, pp. 267–87.

7 Chris Bing, "Command and Control: A Fight for the Future of Government Hacking," *CyberScoop*, April 11, 2018: https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/ (accessed March 29, 2022).

8 Jason Healey, "The Implications of Persistent (And Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5, no. 1 (Oxford, 2019): https://doi.org/10.1093/cybsec/tyz008 (accessed March 29, 2022).

9 Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (London: Hurst & Company, 2016).

it would raise concerns not only in the United States but also across the globe.[10] Furthermore, trying to shape the behavior of actors may not be as effective as planned – both state and non-state adversaries keep on compromising US networks successfully and at a large scale, as demonstrated by the SolarWinds hack and the Colonial Pipeline ransomware attack.

The primary lesson for the EU to learn from the US experience is that it is futile to significantly alter the behavior of adversaries through cyberspace. And yet, the EU's current defensive approach of trying to dissuade adversaries from attacking is futile too. Rather than trying to shape adversary behavior, the EU should *shape the substance of cyberspace itself*, which would, in turn, raise the cost for malicious actors to engage in offensive behavior. The EU doctrine should explain why it is important to tilt the offense-defense balance to the defender's advantage.[11] It should highlight why it is crucial to strengthen the defender in each dyadic relationship with an attacker. This doctrinal thinking can be summed up as *defense superiority* in cyberspace.[12]

Acting upon this doctrine, the EU should follow what this policy brief defines as a strategy to *secure the cyber domain* that focuses on the following:

- Making cyber operations less significant, i.e., reducing the propagation of malware across companies, ministries, and individuals, for example through information sharing
- Decimating the disruptive effects of cyber operations through redundancy
- Limiting the depth of intrusions with tools such as multifactor authentication

This proposed strategy does include some elements of persistent engagement, such as limited cyber operations to disrupt operations. However, those cyber operations are not a priority here, and they are not meant to change adversary behavior or gain relative advantages compared to hostile states. In the securing the cyber domain strategy, cyber operations are only meant to disrupt ongoing malicious operations. Moreover, this strategy differentiates itself from US posture in cyberspace, which encourages malware to be implanted in the critical national infrastructure of an enemy, creating a deterrence mechanism by holding it at risk to discourage attacks above the threshold of armed conflict.[13] The strategy of securing the cyber domain does not subscribe to implanting malware for such a deterrent purpose.

IMPLEMENTING DEFENSE SUPERIORITY THROUGH A STRATEGY OF SECURING THE CYBER DOMAIN

The **doctrine of defense superiority** states that, in many instances, cybersecurity is best achieved through a defensive rather than an offensive posture.[14] What is more, many sophisticated and high-resource cyber operations are already more expensive for the attackers than the defenders.[15] What the EU has failed to do so far is to significantly increase the instances in which the defender enjoys superiority. By increasing the level of cybersecurity systematically throughout the system – in society, the private sector, the government, and the military – in the EU and beyond, the offense-defense balance can be more strongly tilted to the defender's advantage.[16] This strategy goes beyond taking a defensive posture, which is what the EU currently does; it is about changing cyberspace to favor the defense. In this process of enhancing cybersecurity, hostile cyber operations will continue. However, with time, their possibility to affect entire systems and industries will be reduced and their occurrence made more tolerable.

The internet was not built with security in mind, but this can be changed over the medium and long term with a **securing the cyber domain strategy**. To

10 Herb Lin, "A Hypothetical Command Vision Statement for a Fictional PLA Cyber Command," *Lawfare*, October 22, 2021: https://www.lawfareblog.com/hypothetical-command-vision-statement-fictional-pla-cyber-command (accessed March 29, 2022).

11 The doctrine of defense superiority is primarily a descriptive proposal, e.g., the offense-defense balance can be tilted to favor the defender rather than attacker. In contrast, the securing the cyber domain strategy is a prescriptive proposal.

12 Superiority is seen as a degree of dominance. US Cyber Command, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command" (Maryland, 2018): https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf (accessed March 29, 2022).

13 US House of Representatives, "Text – H.R.5515 – 115th Congress (2017–2018): John S. McCain National Defense Authorization Act for Fiscal Year 2019," August 13, 2018: https://www.congress.gov/bill/115th-congress/house-bill/5515/text (accessed March 29, 2022).

14 Harold Abelson et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity* 1, no. 1 (September 1, 2015), pp. 69–79: https://doi.org/10.1093/cybsec/tyv009 (accessed March 29, 2022).

15 Rebecca Slayton, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (2016), pp. 72–109: https://doi.org/10.1162/ISEC_a_00267 (accessed March 29, 2002).

16 David T. Fahrenkrug, "Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy," *4th International Conference on Cyber Conflict*, NATO CCD COE, 2012: https://ccdcoe.org/uploads/2012/01/3_4_Fahrenkrug_AnIntegratedDefensiveStrategy.pdf (accessed March 29, 2022).

achieve this and become more secure, the EU will have to shape not only the cyber-ecosystem within its borders but also the cyber-ecosystem abroad.

More specifically, the strategy should consist of denying cyber operations their significance through these measures, each of which is explained in more detail below:

- Systemic measures to improve cybersecurity
- Strategic cyber capacity-building abroad
- Deception
- Limited cyber operations to disrupt ongoing attacks

Systemic Measures to Improve Cybersecurity

Rather than minimizing the impact of attacks (independently of what adversaries do), the main idea behind current EU regulation is to build up defenses to dissuade adversaries from attacking (deterrence by denial). The way the EU and its member states issue such regulations is piecemeal, often focusing on threats against national critical infrastructure. In no way does this approach follow a comprehensive strategy to make cyberspace defense superior at a systemic level.

With respect to **regulation**, the EU has already been very active with several directives that aim to increase the cybersecurity level in critical sectors such as banking, drinking water, and health care.[17] These industries are now required to conduct risk assessments and report cybersecurity incidents to authorities. In the latest EU directive, new sectors have been added that need to comply with these regulations. Another of the EU's notable regulatory measures is the Cyber Resilience Act, the goal of which is the creation of a shared cybersecurity standard for products related to the Internet of Things (IoT).[18] Major challenges to implementing these regulations are finding the human resources within member states to monitor the cybersecurity standards that are being set for them and setting economic incentives for companies to comply.[19]

The EU and its member states should also commit to strong and ubiquitous encryption and enshrine this in the regulatory environment.[20] Weakening end-to-end encryption, as currently discussed in EU institutions, would weaken cybersecurity for everyone in the EU and give foreign governments even more advantage in their cyber operations, thereby tilting the offense-defense balance further in the attacker's favor. In addition, the EU needs a regulatory framework that incentivizes the diversification of networks. This could be achieved by increasing the number of fiber lines and building resilient industrial and command and control systems that have redundancy mechanisms in place.[21] Yet another way to strengthen cybersecurity throughout the EU's territory would be to further roll out multi-factor authentication, which blocks around 99 percent of the most recurrent attacks,[22] and make it easier to use.

Improving the security of software supply chains should become an integral part of the national security policymaking of the EU and its member states.[23]This could be done by setting up long-term funding to support the security and patching of vulnerabilities of open-source software, which could reduce the frequency of incidents such as the exploitation of a bug in the widely used Log4j.[24] That bug was partly the result of the fact that the library software was only looked after by three volunteer programmers – clearly, they did not have the resources to provide proper security for it. Especially given how many users rely on such open-source software programs, investment in defending them would be a valuable step.

The EU is particularly well suited to shape the cybersecurity landscape around the world as it could start by doing so in its own market of 450 million consumers. While import requirements could induce com-

17 The author alludes to NIS1 and NIS2 directives. European Commission, "Revision of the Network and Information Security Directive: Questions and Answers|Shaping Europe's Digital Future," October 19, 2021: https://digital-strategy.ec.europa.eu/en/revision-network-and-information-security-directive-questions-and-answers (accessed March 29, 2022).

18 Breton, "How a European Cyber Resilience Act Will Help Protect Europe" (see note 1).

19 Timo Kob, "NIS-2 – Gut Gemeint, Nicht Gut Gemacht" [NIS2 – Well Meant, Not Well Done], *Tagesspiegel Background Cybersecurity*, February 7, 2022: https://background.tagesspiegel.de/cybersecurity/nis-2-gut-gemeint-nicht-gut-gemacht (accessed March 29, 2022).

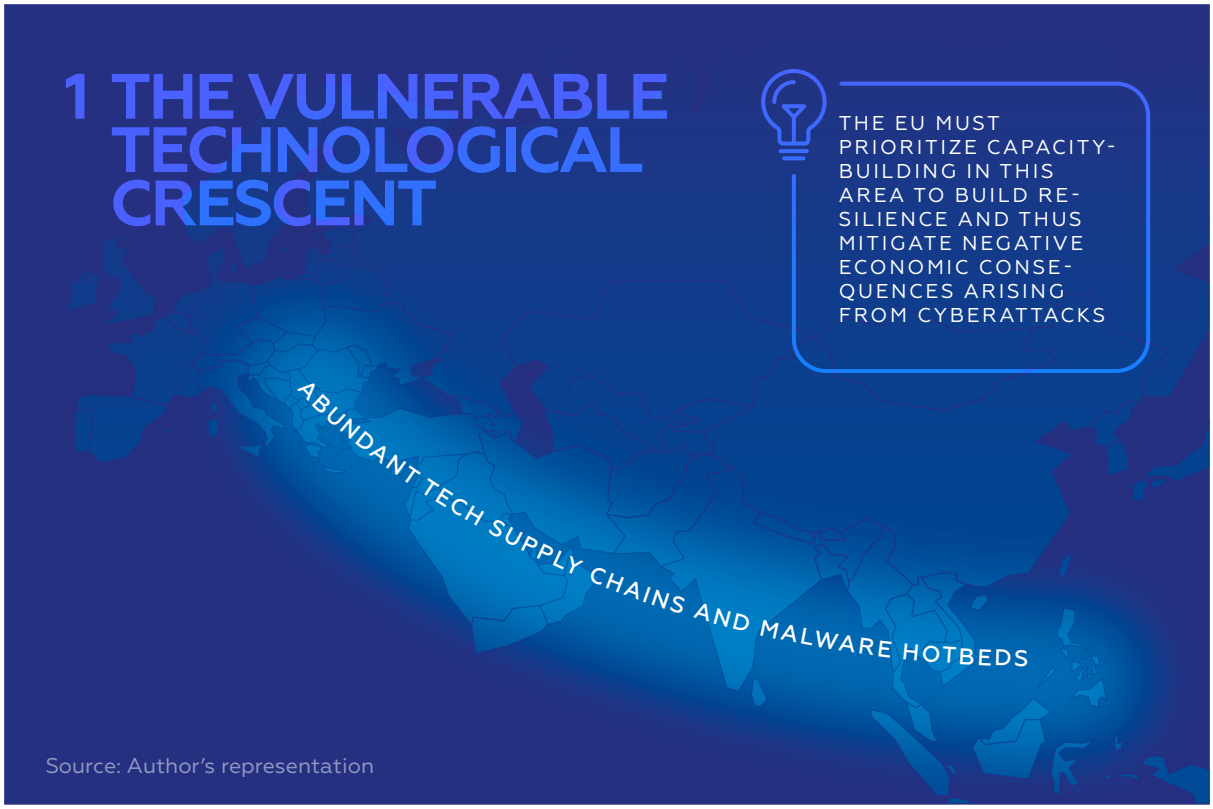
20 Valentin Weber, "How China's Control of Information Is a Cyber Weakness," *Lawfare*, November 12, 2020: https://www.lawfareblog.com/how-chinas-control-information-cyber-weakness (accessed March 29, 2022).

21 Fahrenkrug, "Countering the Offensive Advantage in Cyberspace" (see note 16).

22 Valentin Weber, "The Illusion of 'Responsible' Cyber Offense," German Council on Foreign Relations, October 27, 2021: https://dgap.org/en/research/publications/illusion-responsible-cyber-offense (accessed March 29, 2022).

23 Trey Herr et al., "Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain," Atlantic Council, July 27, 2020: https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/ (accessed March 29, 2022).

24 Sovereign Tech Fund, "Machbarkeitsstudie Zur Prüfung Eines Förderprogramms Für Offene Digitale Basistechnologien Als Grundlage von Innovationen Und Digitaler Souveränität" [Feasibility Study to Examine a Support Program for Open Digital Base Technologies as the Basis for Innovations and Digital Sovereignty], 2021: https://sovereigntechfund.de/SovereignTechFund_Machbarkeitsstudie.pdf; Lucas Ropek, "After Log4j, Open-Source Software Is Now a National Security Issue," *Gizmodo*, January 13, 2022: https://gizmodo.com/after-log4j-open-source-software-is-now-a-national-sec-1848356403 (both accessed March 29, 2022).



panies supplying EU markets to comply with high cybersecurity standards, the EU is unlikely to be able to secure the cyber domain all by itself. It will have to create strategic partnerships with the United States, Taiwan, South Korea, Japan, and other countries to create synergies. For example, while the US might not prioritize resilience in its cyber posture, there is still much space for collaboration, such as in improving the security of open-source software.[25]

Strategic Capacity-Building

At the same time, the EU should engage in strategic cyber capacity-building. This means that it must **establish geographical priorities** as to where it provides financial and expert assistance, i.e., regions from where much of the hardware and software used in the EU originates. The EU must focus its capacity-building efforts on the geographical area spanning Southeastern Europe, the Middle East, and South and Southeastern Asia. This area – which this author has labelled the Vulnerable Technological Crescent (see graphic 1) – is one of the world's most important to the tech sector as it harbors an abundance of technological supply chains.[26] And yet, it remains fundamentally vulnerable. An obstruction of this area would have enormous economic consequences for the EU. Hence, resilience there is of utmost importance.

Countries within this crescent, for example Georgia or North Macedonia, are also frequently used by Russian state actors as testbeds for malicious cyber tools. Hence, building resilience there would allow the EU to get a better grasp on the threats lurking in these systems today that could target EU member states tomorrow. Similar geographical focal points could be envisioned in Southeastern Asia in areas along China's Belt and Road Initiative, which are likely riddled with Chinese malware.[27]

Meanwhile, the EU should anchor its doctrine of defense superiority within its capacity-building programs to promote its worldview among other states. The more states invest resources to implement this

25 The White House, "Readout of White House Meeting on Software Security," January 14, 2022: https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/ (accessed March 29, 2022).

26 The representation of this crescent shows the larger geographical areas of importance and not a specific list of the states that are part of it or not.

27 FireEye, "M-Trends," 2019: https://www.mandiant.com/sites/default/files/2021-09/rpt-mtrends-2019.pdf (accessed March 29, 2022).

doctrine and collaborate with the EU by building capacities to achieve it, the more defense superior cyberspace will become beyond the EU's borders.

Deception

The magnitude of attacks may also be reduced if it takes attackers more effort to identify valuable data and systems.[28] This effect can be reached through deception. Endpoint deception, for instance, involves the **creation of decoy network elements** that are meant to consume the attacker's time and lure them away from real network elements.[29] If one is bolder, one could use honeypots to lure the attacker into downloading malicious software through which the defender could disrupt ongoing attacks on its networks.[30]

Limited Cyber Operations to Disrupt Ongoing Attacks

The issue of conducting cyber operations is entirely left out of both the 2020 EU Cybersecurity Strategy and the EU Cyber Defense Policy Framework that was updated in 2018.[31] The EU Mutual Defense Clause allows for assistance between states in the case of a cyberattack that is severe enough in character, but it omits defense below this threshold, which is the primary focus of this policy brief.[32] The *usefulness* of such capabilities is raised in the European Parliament resolution of October 7, 2021, on the state of EU cyber defense capabilities; it states that "cyber defense is more effective if it also contains some offensive means and measures, provided that their use is compliant with international law."[33] Those notions are vague and also do not address the challenge of responding to less severe cyber operations.

EU member states should have capabilities for conducting cyber operations to disrupt ongoing attacks.[34] These could include taking down botnets or ransomware operations when states that harbor such infrastructure remain uncooperative. In this way, malicious cyber operations are prevented from escalating and producing significant effects. The response to such attacks should be bound by time – for example, it should not be possible to use offensive cyber means a year after an attack took place.

What is more, **retaliation and the incurrence of costs should be limited to other domains**. Punishment of cybersecurity or technology companies should be imposed through economic sanctions, for instance, rather than a cyber retaliation. This is due to what appears to be the ineffectiveness of significantly changing adversary behavior in cyberspace through cyber means, as illustrated in the introduction. As a result, punitive measures outside the cyber domain should be prioritized. Those are illustrated in the EU Cyber Diplomacy Toolbox and involve sanctions and public statements. While their effectiveness can be questioned as both are often imposed too late and have too mild an effect, they at least allow for clear signaling to an adversary that one disapproves of malicious cyberattacks. This showing of disapproval is often difficult to achieve in cyberspace, due to the secretive and often anonymous nature of the cyber domain.[35]

WHY DEFENSE SUPERIORITY IS THE RIGHT DOCTRINE FOR THE EU

Coherence in Cyber Defense and Diplomacy

The goal of securing the cyber domain both at home and abroad translates into coherence in cyber defense and diplomacy. In the United States, persistent engagement and diplomacy are often at odds, because the former inherently has an inclination toward the weakening of cyber systems (maintaining backdoors) and offensive behavior. On the other hand, US diplomats promote strong systems that assure privacy and the freedom of expression

28 Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (April 3, 2015), pp.316–48: https://doi.org/10.1080/09636412.2015.1038188 (accessed March 29, 2022).

29 CYBERTRAP, "Deception Technology," 2022: https://cybertrap.com/en/ (accessed March 29, 2022).

30 Gartzke and Lindsay, "Weaving Tangled Webs" (see note 28).

31 Council of the European Union, "EU Cyber Defence Policy Framework," November 19, 2018: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf (accessed March 29, 2022).

32 The EU Mutual Defense Clause is enshrined in Article 42.7 of the Treaty on the European Union from 2007. European Parliament, "Mutual Defence Clause": https://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede200612mutualdefsolidarityclauses_/sede200612mutualdefsolidarityclauses_en.pdf (accessed March 29, 2022).

33 European Parliament, "Texts Adopted – State of EU Cyber Defence Capabilities," – October 7, 2021: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0412_EN.html (accessed March 29, 2022).

34 For a discussion of response options for states under the current framework of international law see Isabella Brunner, Erich Schweighofer, and Jakob Zanol, "Malicious Cyber Operations, 'Hackbacks' and International Law: An Austrian Example as a Basis for Discussion on Permissible Responses," *Masaryk University Journal of Law and Technology*, 2020: https://heinonline.org/HOL/LandingPage?handle=hein.journals/mujlt14&div=15&id=&page= (accessed March 29, 2022).

35 Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, Massachusetts: Harvard University Press, 2020).

2 – THE CYBER POSTURE OF THE UNITED STATES FOCUSES PRIMARILY ON PUNISHMENT AND FRICTION

Doctrine	Persistent engagement
Doctrinal belief	The United States is in constant engagement with adversaries in cyberspace and needs to use the offensive advantage
Strategy	Department of Defense Cyber Strategy (2018)
Rationale behind the strategy	Through constant presence in enemy networks, malicious operations can be preemptively identified, halted, and deterred
Strategy for addressing operations above the threshold of armed conflict	Offensive cyber operations are conducted to cause a deterrent effect (punishment), e.g., malware implants in the critical national infrastructure of an adversary (see note 13)
Strategy for addressing operations below the threshold of armed conflict	Offensive cyber operations are conducted to cause friction and disrupt enemy attack infrastructure (defending forward); the goal is to change adversary behavior

Source: Author's own compilation

(e.g., Signal Messenger) and restraint on offensive cyber behavior (norms of responsible behavior in cyberspace).

The EU's defense superiority doctrine would avoid these pitfalls, since it is based on the premise that defense provides the best cybersecurity. Together, the defense and diplomatic establishments could implement a strategy that follows this worldview. While law enforcement and intelligence agencies – including in EU member states – have historically pushed for a weakening of encryption to fight crime and terrorism, encouraging signals come from Germany, where the right to encryption is anchored in the coalition agreement of its new government.[36]

A Proper Use of Military Capabilities

In the United States, the US Department of Defense's cyber budget is larger than that of the Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Department of Justice combined.[37] These vast resources lead to the military being tasked with civilian responsibilities that it usually should not be considered for.

Meanwhile, in Europe, the Dutch have been thinking out loud about using the military to fight ransomware attacks; like the United States, Germany has already done so.[38] The rationale for deploying the military at home in such cases risks unnecessarily militarizing cyberspace since other agencies could do the job just as well. What is more, it drains resources away from the military that it could use for defending its own networks.

The defense superiority doctrine sees cyberspace as a largely civilian space and suggests a wider dissemination of resources to this space when it comes to

36 Valentin Weber and David Hagebölling, "G7-Präsidentschaft: Warum Sich Deutschland Für Starke Verschlüsselung Einsetzen Muss" [G7 Presidency: Why Germany Must Commit to Strong Encryption], German Council on Foreign Relations, February 11, 2022: https://dgap.org/de/forschung/publikationen/g7-praesidentschaft-warum-sich-deutschland-fuer-starke-verschluesselung (accessed March 21, 2022).

37 Gavin Wilde, "On Ransomware, Cyber Command Should Take a Backseat," *Just Security*, November 30, 2021: https://www.justsecurity.org/79361/on-ransomware-cyber-command-should-take-a-backseat/ (accessed March 29, 2022).

38 Oliver Noyan, "German County Targeted by Ransomware Asks Military for Help," *Euractiv*, July 27, 2021: https://www.euractiv.com/section/cybersecurity/news/german-county-targeted-by-ransomware-asks-military-for-help/; Erica Lonergan and Lauren Zabierek, "Cyber Command Is in the Ransomware Game—Now What?", *Lawfare*, December 16, 2021: https://www.lawfareblog.com/cyber-command-ransomware-game%E2%80%94now-what (both accessed March 29, 2022).

3 – THE CURRENT STRATEGY OF THE EUROPEAN UNION FOCUSES ON DENIAL AND PUNISHMENT ABOVE THE THRESHOLD OF ARMED CONFLICT

	CURRENT	PROPOSED
Doctrine	None	Defense superiority
Doctrinal belief	None	The offense-defense balance in cyberspace can be tilted to favor the defending side
Strategy	EU Cybersecurity Strategy (2020)	Securing the cyber domain
Rationale behind the strategy	Deter severe malicious activities through denial and punishment	Limit the significance and impact of malicious cyber operations by systematically securing the technical infrastructure of cyberspace and conducting limited cyber operations to disrupt ongoing attacks
Strategy for addressing operations above the threshold of armed conflict	• Punishment through the EU Diplomacy Toolbox • Denial through regulation, for example the NIS2 directive and the Cyber Resilience Act	Turning cyberspace into an environment that favors the defending side: • Systemic measures to improve cybersecurity • Strategic capacity-building abroad • Deception • Limited cyber operations to disrupt ongoing attacks
Strategy for addressing operations below the threshold of armed conflict	None	

BECAUSE THE EU CURRENTLY HAS NO STRATEGY FOR CYBER OPERATIONS BELOW THE THRESHOLD OF ARMED CONFLICT, IT SHOULD FOCUS ON PRIMING ITS TECHNICAL INFRASTRUCTURE FOR DENIAL IN THIS KEY AREA

Source: Author's own compilation

cybersecurity. Civilian agencies and actors should receive a good portion of the resources invested into making cyberspace more secure, thereby avoiding overreliance on the military to secure the domain. Well-defined guardrails should be put into place to allow for specific cases of military protection of domestic civilian networks.

Arguing for a cyber strategy focused on defense might seem counterintuitive, especially in light of Russian President Vladimir Putin's war in Ukraine, which dangerously exposes the EU's eastern flank. One might argue that a cyber power with highly developed offensive capabilities would have a decisive advantage in such a conflict and that the EU member states should prioritize investing in such capabilities. But as of now, it seems that offensive cyberattacks have had few sizeable impacts that would support the Russian military invasion. As far as public sources reveal, Russia has largely relied on traditional missiles to blow up critical infrastructure rather than use cyberattacks to disable it.[39] In short, the most important aspects in conventional war are having hard power in the form of tanks and fighter jets at the ready and ensuring the continued operation thereof, shielding them – as well as the satellites and other communications infrastructure that they rely on – from cyberattacks.

39 Thomas Rid, "Why You Haven't Heard About the Secret Cyberwar in Ukraine," *The New York Times*, March 18, 2022: https://www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html (accessed March 29, 2022).

CONCLUSION: PEEKING INTO THE FUTURE

One should not engage in wishful thinking. Defense superiority will not dissuade hostile states from attacking in the cyber realm in the short and medium term. Europeans doubling down on defense might even incite additional malicious cyberattacks to test what the new strategy and doctrine mean. The EU will have to impose proportionate sanctions to punish individuals, entities, and industries involved in these attacks while at the same time persist in securing the cyber domain.

The potential advantage for Europe in being the first one to adopt this strategy is that, in the medium and long term, attacking states such as China, Russia, Iran, and North Korea may find it harder to lead cyber operations against the EU while they will remain vulnerable. This is because their authoritarian governments rely on weakened security and backdoors littered across their territory that provide the regimes with full situational awareness of financial and economic systems, social networks, and private messages. In China, commercial cryptography is intentionally weakened. To give an example, software that Chinese companies use to file taxes is presumed to contain vulnerabilities to allow for government snooping.[40] While these vulnerabilities may apply to software that is predominantly used in China, these weaknesses may also spill over to the EU when exported. Therefore, to turn cyberspace truly defense superior, the EU and its member states must not only get allies and partners onboard but also authoritarian countries – principally among them, China.

ACKNOWLEDGEMENTS:

The author would like to thank James Shires, Tyson Barker, Roderick Parkes, and Jantje Silomon for their immensely helpful feedback. All errors are the authors'.

40 Weber, "How China's Control of Information Is a Cyber Weakness" (see note 20).

DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
@dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP).

DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

Publisher
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2198-5936

Editing Helga Beck

Layout Luise Rombach

Design Concept WeDo

Author picture(s) © DGAP