SWP Comment
NO. 48 SEPTEMBER 2023

Shifting Paradigms in Europe's Approach to Cyber Defence

Ambitions to Disrupt Malicious Cyber Activity Need to Protect Norms as Well as Networks

Annegret Bendiek and Jakob Bund

As high-level European Union (EU) policy documents call for investment in active cyber defence capabilities, the legal and political powers for their use remain ill-defined. To demonstrate their commitment to principles of responsible state behaviour and due diligence, the EU and its member states have a duty to establish the normative foundations for the use of active cyber defence measures ahead of their deployment, while carefully managing the risk of a gradual militarisation of the cyber and information domain.

In November 2022, Australia brought together its Federal Police and the Australian Signals Directorate in a Joint Standing Operation (JSO) dedicated to disrupting cyber criminals. In the months prior, hackers had attacked Medibank — Australia's largest nationwide health insurer — and one of the country's leading telecommunications providers, Optus. On a large scale, the personal and sensitive health data of around 40 per cent of the Australian population was stolen and published. In a break with traditional methods of policing, the hundred-strong JSO no longer reacts after crimes have been committed, but instead tries to prevent cyber criminals from committing their deeds beforehand.

Incidents like those experienced by Australia illustrate the increasing importance of mitigating cyberattacks and cooperating internationally to hold cyber criminals accountable. The latest developments were also in the background of the consultations for Germany's National Security Strategy, which, in addition to considerations on strengthening resilience, also included active cyber defence measures to prevent damage from cyberattacks in advance. This would require an amendment to Germany's Basic Law, which the Federal Government is also seeking. Germany's first National Security Strategy, presented in June 2023, commits it to reviewing the existing powers for cyber defence and the capabilities required for this. Recognised legal principles of due diligence, proportionality of countermeasures and international norms on responsible state behaviour in cyberspace are guiding action in this regard. The document

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

reiterates that the German government is ruling out "hackbacks" as a means of cyber defence. In response to a parliamentary inquiry, the government noted earlier that the term itself lacks a clear definition. The German cyber ambassador, Regine Grienberger, separately pointed out the high legal hurdles for the proactive disruption of cyber threats. A prerequisite for this is the reliable and robust attribution of attacks, based on the identification of the attacker according to technical, political and legal standards. The enforcement of existing law inevitably also depends on having the necessary cybercrime prevention and law enforcement capabilities in place.

NATO's new Strategic Concept, adopted in 2022, describes cyberspace as being continuously contested. David van Weel, Deputy Secretary General for Emerging Security Challenges, recently outlined that this assessment applies regardless of whether one is in an armed conflict situation. At the Alliance summit in Vilnius in July, NATO member states therefore backed a new cyber defence concept to ensure civil-military cooperation at all times — "through peacetime, crisis and conflict" — and facilitate the involvement of private-sector actors.

Cyber defence considerations in the Alliance, at EU level and also in some EU states are moving away from a reactive understanding and towards a proactive approach against threats. Central to these deliberations is how member states define the active cyber defence responsibilities that they assign to civilian agencies — including law enforcement — and their distinction from responsibilities of the military. Do these developments point to a more fundamental paradigm shift in the European approach to cyber threats — from a reactive to a more proactive defence posture? A review of emerging state practice identifies key questions that Europe needs to work through, as close partners such as the United States (US), the United Kingdom (UK) and Australia are already engaging in disruptive defence operations to frustrate threats. Due diligence remains a fundamental prerequisite in this endeavour.

Ambiguous definitions

In the November 2022 Communication on an EU Cyber Defence Policy, the European Commission called on member states to develop capabilities across the full spectrum of cyber defence, including active measures. The Council Conclusions on Cyber Defence Policy of May 2023 further emphasise the importance of civil-military cooperation. Capabilities for early detection, defence against and deterrence of cyber threats would have to complement the portfolio of defence instruments. While underscoring that these are national competences — with the decision and responsibility for the deployment of cyber defence measures lying squarely with the governments of member states — the Council pointed to the defensive character of these measures. Which techniques and procedures member states might explore as part of their active cyber defence ambitions is left open in the Conclusions. Instead, the member states are called upon to specify their own goals and outline measures for achieving them. The methods of active cyber defence documented so far through policy papers, interviews and limited examples from state practice include the diversion of harmful data traffic, the disabling of botnets and the takeover of servers or internet domains by law enforcement agencies to strip attackers of control over their infrastructure. The defence tools also include the identification and deactivation of malware in computer systems and intervention in attacking IT infrastructure outside the systems of the affected victims. In this vein, active cyber defence may include disinformation campaigns, the manipulation of foreign media, the electronic disruption of servers and the halting of data traffic abroad.

The principle of due diligence

The German government, EU member states and the EU are guided by the requirements of "due diligence" in the implemen-

tation of their cybersecurity strategies. This obligation binds states in peacetime to ensure that no activities emanating from their territory violate the rights of other states. In its cybersecurity strategies, the EU points out that the protection of computer systems and networks is essential for a modern, high-tech and digitised industrial state. To this end, the resilience of infrastructure, the ability to defend against and detect (also state-directed) cybercrime and awareness of disinformation campaigns are the focus of enhanced defence efforts.

The EU and Germany pursue a defensive cyber security strategy based on international agreements. The concept of due diligence is, however, not per se in conflict with active cyber defence. Yet, intervening in adversary cyber operations poses new challenges to state due diligence in peacetime, even as such actions may be justifiable in terms of defence against "imminent danger". International norms act as anchor points for the design of active cyber defence measures. Proactive cyber defence therefore requires the disclosure of norm-violating behaviour in order to justify in comparable cases that the intervention was carried out to avert danger or in the context of an imminent threat. US authorities have repeatedly demonstrated the willingness to make operational insights public through indictments of threat actors, even where those responsible are likely to remain beyond prosecution.

Revealing such information as part of attribution efforts signals a commitment to hold threat actors accountable to allies. Steps in this direction have strengthened an international "attribution coalition" among EU and NATO states and international partner countries. To clearly define what is considered acceptable behaviour, details on the powers and mandates of the new authorities must be provided, especially in the case of active defence initiatives. Exposing adversary activity and distinguishing "blue actions" from hostile operations are instrumental for not upending progress in shaping the very norms that provide legitimacy for disrupting threats. At the same time, states will have to find a delicate balance in their public reporting to protect sources and methods and to avoid undermining their ability to conduct future operations.

State practice of active cyber defence

The US Department of Defence transitioned to a new approach to cyber defence in 2018. In the attempt to "defend forward", US Cyber Command, under this doctrine, focusses on countering threat activities as close to their source as possible to avert damage before it can occur and intercept hostile actors. It pursues this approach through "persistent engagement" — the targeted disruption of cyber threats and the degradation of an adversary's capabilities — in order to impose costs on attackers and influence behaviour that has proven difficult to shape through other instruments, or otherwise could only be addressed after the fact. The National Cyber Security Strategy published in March 2023 develops this approach further for civilian agencies. The document establishes a stand-alone pillar of disrupting and weakening threat actors. According to General Paul Nakasone, head of US Cyber Command and director of the National Security Agency, the US Department of Defence's new cyber strategy — adopted two months later and classified — builds on the change of course made in 2018. While the Department's fourth edition, the 2023 strategy, is the first to be "informed by years of significant cyberspace operations".

In contrast to the rise in pronouncements about active cyber defence initiatives, little is known about the scenarios for their deployment. Even for the US, which has been among the most transparent about its willingness to use offensive capabilities, public cases and operational details are sparse.

The first known case of active intervention in malicious cyber activity by US Cyber Command was aimed at disconnecting the Trickbot botnet from command-and-control servers in autumn 2020 to counter a pos-

sible ransomware campaign in the run-up to the US elections.

The Cyberspace Solarium Commission, a body set up by the US Congress to develop a concept for defence against serious cyberattacks, proposed an expanded interpretation of "defend forward" in 2020. According to this interpretation, consistent implementation of the doctrine no longer only drew on military instruments, but all state capabilities (diplomacy, regulatory powers, etc.), especially to make intelligence on threat activities available to potential targets, thereby contributing to their resilience. The Commission's interpretation indicates that a robust "defend forward" policy will also be measured by whether and to what extent it contributes to strengthening international norms of behaviour. In the public summary of its new cyber strategy, the Department of Defence recognises its capabilities are most effective when deployed as part of an integrated approach, though it does not address other instruments in further detail.

Countering attack activity is only one step in bringing about a change in adversary behaviour. Demonstrating the ability and determination to continue to do so to potential attackers underwrites these signalling efforts. According to General Nakasone, in response to Russia's invasion in the spring of 2022, the US conducted offensive cyber operations in support of Ukraine, in addition to defensive ones.

Other states also intend to use operational influence capabilities to actively disrupt malicious cyberattacks. In addition to the aforementioned deployment of the Australian JSO for cyber defence, the Australian government announced earlier this year that it will triple its investment in offensive cyber defence capabilities.

The UK has made public a range of assistance measures since Russia's invasion of Ukraine in February 2022. The programme includes supporting critical infrastructure and Ukrainian government agencies in dealing with cyber incidents, assistance to avert sabotage attempts against the power supply, forensic intelligence, and access to security solutions to protect high-value targets from future attacks. Not all of these measures have received full endorsement among EU member states. Nor are the technical cyber capabilities that are necessary for more active support roles equally distributed among EU member states. Ukraine's resilience to Russia's attacks suggests that it may have benefited from forward-leaning cyber defence measures. Kyiv's proactive calibration of defence efforts relied, among other things, on the results of Hunt Forward Operations (HFOs), which were conducted by US Cyber Command and Ukrainian partners between December 2021 and March 2022.

Hunt Forward Operations as active threat prevention

As interpreted by US Cyber Command, HFOs are defensive efforts in which internal protection teams — at the request of partner states — scan networks on site for malware in order to detect new attack patterns early on and close security gaps and backdoors. The key advantage of the hunt-forward approach, according to General Nakasone, is that threat actors and their tools can be detected in advance. To date, US Cyber Command has conducted more than 50 HFOs with at least 23 countries. Partners have included several EU member states and NATO allies, including Albania, Montenegro and northern Macedonia. Shortly after Russia's invasion of Ukraine in February 2022, teams were deployed to Lithuania and later Latvia. European partners have thus not only already participated bilaterally in HFOs but are directly requesting deployments in their networks.

Germany and other EU states interested in exploring HFOs may engage in three separate ways. A joint deployment in their own networks makes it possible to draw on the analytical capabilities of international partners in the reconnaissance of attack activities to a degree that could not be achieved through an exchange of information only.

In the opposite direction, such an operation in support of international partners

can provide new knowledge about tactics and attack tools that are being tested. This knowledge expands the possibilities to prepare for attempted attacks and, ideally, to prevent them before they can cause damage.

European states are faced with the question of whether the development of anticipatory capabilities requires similar programmes under their own leadership. Without committing member states to participate directly, a European project could be set up with the aim of maintaining independent capabilities and having clarified operational modalities in case of need. The EU's Permanent Structured Cooperation (PESCO) provides an existing framework within which member states could invest in HFO resources.

European reactions

A strategic reorientation towards active cyber defence is politically controversial among member states. The head of the French Cyber Defence Command, General Aymeric Bonnemaison, expressed reservations to this effect in a hearing of the National Assembly in December 2022. In Bonnemaison's rendition, even defensive missions that serve to scout out adversary activity in allied networks remain aggressive. Support of this kind, especially for Eastern European countries, while providing reassurance, presupposes far-reaching access to the networks concerned and requires a strong operational presence — which in Bonnemaison's view would make accompanying diplomatic engagement and capacity-building on the ground indispensable. To address these points, the French cyber commander floated the idea of a European cyber intervention group that offers assistance similar to US-led HFOs. Even for countries that stand to benefit from this assistance in light of long-term security challenges, it could require temporary, far-reaching access to their sensitive networks.

At a low-threshold level, EU Cyber Rapid Response Teams (EU-CRRTs) already offer support to third countries in monitoring and combating cyber threats. A group of eight member states has built up the necessary capabilities within PESCO. The EU-CRRTs, comprising eight to twelve national experts, were the first operational units under PESCO. The states participating in the PESCO project alone decide on mobilisation. Although operational since 2019, an EU-CRRT was activated for the first time at the request of Ukraine in February 2022, shortly before the start of Russia's war of aggression. After initial efforts to deploy forces both onsite and remotely, Russia's assault necessitated a change of course towards fully virtual support. The deployment of another force to Moldova is reportedly in preparation. The EU also delivered equipment for a cyber lab to the Ukrainian armed forces in December 2022 under the European Peace Facility. The lab will serve as a training environment to build additional capabilities through real-time simulations to detect, understand and defend against attempts to penetrate Ukrainian networks.

Normative foundations are missing

Emerging state practice by the US, the UK and Australia outlines the rationale and expected contributions of active defence measures in containing threats. Any deploying state has a duty to ensure that such deployments are appropriate and comply with accountability obligations. Any consideration of active cyber defence first needs to define which active measures should be meaningfully pursued by which domestic actors and in which international or European partnerships. It also requires clarity on how these actions address security concerns that otherwise lack remedy and how they can contribute to the resilience of partners. In an increasingly volatile strategic environment for the EU, the potential of active cyber defence increasing the costs for engaging in malicious activity may be appealing, but needs to be tied to the definition of preconditions regarding transparency,

legitimacy and accountability of such operations, at least in the following points:

- Active defence measures should be closely linked to firm operational principles and a careful impact assessment. This places high demands especially on explaining the necessarily forward-looking character of defensive and at the same time disruptive actions. Their purpose of disrupting offensive operations must be clearly distinguished from actions designed with the intention to cause harm. Considerations of the effects must not be limited to influencing an adversary's cost-benefit calculations but should also include downstream consequences for global stability in the cyber and information space. Similarly, there is a need for an evaluation framework and metrics that allow for an integrated, strategic, operational and tactical assessment beyond the mere number of operations conducted or their immediate tactical effects.
- The Solarium Commission emphasises that the tactical and operational implementation of the "defend forward" policy includes deployment in networks of partners and allies if disruptive measures can only achieve their goal in this way. As the example of the deletion of propaganda material of the "Islamic State" from a German server shows, such cross-border active cyber defence interventions require a shared situational understanding and advance communication between the countries concerned. Against this backdrop, the Commission pointed out that such actions should be carried out with the support of allied partners whenever possible. Regardless of their willingness to develop active cyber defence capabilities, from the US perspective this requires close coordination with allies and other like-minded governments. On the EU side, the planned Cyber Defence Coordination Centre (EUCDCC) could in the future be a platform for coordination with international partners. At least initially, the EUCDCC's efforts to establish a situational awareness of ongoing cyber operations will focus on Common Security and Defence Policy missions and operations.
- Existing formats for sharing voluntarily provided cyber capabilities, such as NATO's SCEPVA programme (Sovereign Cyber Effects Provided Voluntarily by Allies), show how difficult it is to put cooperation in this area into practice. Participating actors are concerned about revealing the building blocks of their own capabilities. In practice, therefore, capabilities are not shared but deployed at the request of allies. For active defence, these hurdles to capability-sharing sit even higher, considering its premise of the continuous and proactive engagement of threat activity. Active defence takes aim at activities below the threshold of an armed attack. Rules of engagement are therefore much broader in scope than for SCEPVA, which is limited to alliance operations and missions. These developments might increase the political pressure to be able to pursue active cyber defences, at least to some extent, or else risk falling behind. The development of national capabilities raises questions about the possible displacement effects that simply push malicious activities — if these are not target-specific (e.g., ransomware, certain types of industrial espionage) — to the next low-hanging target. Such crowding-out effects risk disruptive approaches evolving into "beggar-thy-neighbour" policies, whereby countries that choose not to respond with disruptive means may find themselves exposed to concentrated threat activity. An example of this is Australia, whose motivation for establishing the JSO was to ensure that it did not present itself as a soft target.
- Information on how the new active cyber defence powers are exercised should be an integral part of a shift in policy and posture. Detecting adversary activities and distinguishing between allied actions and hostile operations are important to demonstrate responsible behaviour and the protection of norms. A com-

mon understanding of active cyber defence measures can only be achieved if states link both disrupted offensive operations and the defensive measures deployed for their disruption to discussions on state behaviour in cyberspace. The public disclosure of "defend forward" operations does not necessarily conflict with protecting sources and methods. On the contrary, transparency about the rationale, the objective and the achieved effect of active defence measures can strengthen the acquis of norms and support the declaratory doctrine. Although there may be cases of operational disruptions to consider in which adversaries do not suspect outside interference, a general presumption that communications on these points routinely depend on disclosing intelligence assets sells short how far public accounts have come.

- Similar mechanisms for responsible transparency are already in place for the proactive use of FBI authorities to delete pre-positioned malware — in these cases the underlying affidavit usually is made public.

A UK National Cyber Force (NCF) report published in early April 2023 assesses active cyber defence as an expression of the responsible exercise of "cyber power". The paper outlines a framework for engaging in disruptive measures while clearly upholding and reinforcing internationally recognised norms and international law. To this end, the NCF paper sketches out a roster of operational prerequisites and identifies indicators for assessing active cyber defence measures in terms of their impact and stabilising influence. In the absence of concrete operational examples, however, how this framework is applied to ensure that operations are conducted according to its "responsible", "precise" and "adapted" standards remains unclear.

In this context, the document points out that transparency with the public is an essential building block of the NCF's "licence to operate". The paper links this provision, among other things, to the additional financial resources that the UK government has dedicated to the development of cyber capabilities.

A critical consideration for ensuring legitimacy and accountability not directly referenced in the document is the forward-leaning character of active cyber defence measures. This expansion of the scope of action is becoming apparent in Germany, not least because of the intended amendment of the Basic Law to grant new authorities. An informed public discourse about any potential extension of powers only gains in importance with respect to the claim that corresponding capabilities are to be deployed in a democratically supported and responsible manner.

For close to a decade, the US has detailed the responsibilities of individual operators and the timing of their actions in indictments and in cooperation with European partners in the form of notices about sanctions. Indeed, efforts to publicly attribute responsibility for cyberattacks have laid the groundwork for the imposition of costs on which any endorsement of active defence would have to stand. As part of their respective cyber defence doctrines, states need to consider under which circumstances information about the use of active defence measures can be made public, especially where such information is already known to the adversary. Such data also provide the feedstock for evaluating whether active defence meets its stated purpose.

A paradigm shift in the strategic culture of European cybersecurity from a reactive to a defensively designed active cyber defence requires critical engagement with the issues raised above. The development of tools for evaluating such missions — in particular assessing the risks of conflict escalation, collateral damage and inadvertent consequences — must be designed into the deliberations about extended powers from the very beginning. European cybersecurity must be measured against its own due diligence principles. A paradigm shift from reactive to active cyber defence is only

justifiable with democratic support. At the foundation of this approach is a public understanding of the strategic environment, and by extension of the conditions that shape cyberspace as a permanently contested field of conflict. Empirically driven cyber conflict and peace research can be a valuable resource in this communication effort. Public data collection to track the development of cyber threats and state responses, as conducted by the European Repository of Cyber Incidents (EuRepoC), can make an important contribution towards ensuring that cyber defence considerations are discussed responsibly and democratically supported.

The online version of this publication contains functioning links to other SWP texts and other relevant sources.

SWP Comments are subject to internal peer review, fact-checking and copy-editing. For further information on our quality control procedures, please visit the SWP website: https://www.swp-berlin.org/en/about-swp/quality-management-for-swp-publications/

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1861-1761
ISSN (Online) 2747-5107
DOI: 10.18449/2023C48

(English version of SWP-Aktuell 49/2023)

Dr Annegret Bendiek is Deputy Head of the EU/Europe Research Division at SWP.
Jakob Bund is an Associate in the EU/Europe Research Division at SWP.
This SWP Comment is based on research conducted by the European Repository of Cyber Incidents (EuRepoC), a research consortium funded by the German Federal Foreign Office and the Ministry of Foreign Affairs of Denmark where Annegret Bendiek is Principal Investigator and Jakob Bund is Researcher.