IAI PAPERS 21 | 05 - FEBRUARY 2021

© 2021 IAI

ISSN 2610-9603 | ISBN 978-88-9368-176-6

Istituto Affari Internazionali

Cyber Defence in NATO Countries: Comparing Models

by Alessandro Marrone and Ester Sabatino

ABSTRACT

In 2016 NATO recognised cyber as a domain comparable to the air, land and sea ones, in consideration of the growing number of cyberattacks and of their negative impact on the cyberspace, as well as on the "real world". Both NATO and its member states have launched initiatives to better tackle the cyber challenge both operationally and in terms of capability development. Nevertheless, among major NATO's members a common approach to cyber defence is still missing, thus generating a division among countries that pursue a more active defence – US, UK and France – and those that prefer a more defensive approach – Germany and Spain.

keywords

Cybersecurity | NATO | USA | United Kingdom | France | Germany | Spain

Cyber Defence in NATO Countries: Comparing Models

by Alessandro Marrone and Ester Sabatino*

Introduction

The proliferation of cyberattacks has generated growing attention from NATO and its member states to the modalities and approaches to effectively ensure cyber defence. The Atlantic Alliance has recognised the cyberspace as a domain, thus making cyberattacks a case for collective defence pursuant to article 5 of the Washington Treaty. In order to ensure a proper defence of its member states, NATO has adopted policies and action plans, establishing committees, agencies and operational centres with the purpose of integrating the cyber domain in both operations and capability development of allies. Nonetheless, the recent recognition of the domain does not allow yet for a single approach to cyber defence that is performed differently in major NATO's countries, and that can be categorised in countries that pursue a more active defence and countries that, instead, prefer a more defensive approach.

Among the former, the United States has established a Cyber Command comparable to the air, land and sea counterparts, in order to ensure the persistence of operations and the maintenance of the engagement through an articulated campaign of seamless defensive and offensive actions. Similarly, the United Kingdom has made public that the development of national capabilities to be employed in the cyber domain also include offensive capabilities, with the possibility of extending the damage to the "real world". Such a proactive approach to cyber defence constitutes the basic understanding also of France, where, in 2018, the Secretary-General for Defence and National Security was tasked with developing a strategy to counter cyber threats, which encompasses both the offensive capabilities – information gathering and attack operations – and the defensive ones.

* Alessandro Marrone is Head of the Defence Programme of the Istituto Affari Internazionali (IAI). Ester Sabatino is a Researcher in the IAI's Defence Programme.
This is the translation of a paper published for the "Osservatorio di politica internazionale" – a collaborative project of the Senate of the Republic, the Chamber of Deputies and the Ministry for Foreign Affairs and International Cooperation, with influential scientific contributions. The original version is *La difesa cibernetica nei Paesi NATO: modelli a confronto*, Rome, Senate, December 2020 (Approfondimento No. 164), http://www.parlamento.it/documenti/repository/affariinternazionali/osservatorio/approfondimenti/PI0164.pdf.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

As for the countries keener on a more defensive approach, Germany is strengthening the infrastructures previously developed at the level of single services, with the purpose of securing a single joint centre for the defence of German institutional networks. However, the German armed forces (*Bundeswehr*), in order to operate on the national territory, need to comply with national and international legislation regulating military activities – with all limitations that come with it. Finally, in Spain, the Joint Cyberspace Command responsible for executing actions linked to the protection of the armed forces' digital infrastructures and systems, performs the kind of response also considering the magnitude of the damage possibly caused by a cyber-attack.

Despite differences in approach, shared necessities exist and attain mainly to the need to have an internationally shared regulatory and doctrinal framework, that allows also for a better integration of the cyber element in national and allied command structures. The recent recognition of the cyber domain requires NATO and its member states also to prioritise a comprehensive approach that takes into consideration the wider concept of resilience, foreseeing a strategic collaboration with enterprises and research entities.

1. The NATO framework

1.1 An evolving approach, strictly linked to collective defence

The Atlantic Alliance's approach towards cyber defence has evolved significantly over the past fifteen years, enhancing its importance as an element which can contribute substantially to all three "core tasks" established by the current Strategic Concept: collective defence, crisis management operations and cooperative security.[1] In particular, it has been acknowledged *de facto* that a cyber-attack can cause damage comparable to that of an armed attack, and thus become a case for collective defence pursuant to article 5 of the Washington Treaty.

The 2008 summit meeting of Heads of State and Government had already adopted a first Policy on Cyber Defence, which then took a leap forward in the 2014 summit with the Enhanced NATO Policy on Cyber Defence.[2] In the subsequent Warsaw Summit in 2016, allied countries recognised cyberspace as a domain, thus equating it to the other conventional military domains – land, sea and air. The Warsaw Summit also led to the signing of the Cyber Defence Pledge,[3] aimed at establishing a common platform to improve national defence and resilience capabilities vis-à-

[1] NATO, *Strategic Concept 2010*, 19 November 2010, https://www.nato.int/cps/en/natohq/topics_82705.htm.

[2] Stefano Mele, "La strategia della Nato in ambito cyber", in *Europa Atlantica*, 3 June 2019, https://wp.me/pabS04-e4.

[3] NATO, *Cyber Defence Pledge*, 8 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

vis a cyber-attack. Subsequently, several action plans have been adopted in order to implement the commitments made with the Cyber Defence Pledge. The allied commitment focuses on the development of defensive capabilities, following article 3 of the Washington Treaty concerning individual and collective capacity to resist an armed attack.[4] Such a focus matches the great importance attached to cyber-attacks, deemed ever more frequent, complex and destructive,[5] to the extent that they can trigger article 5,[6] so much so that in the 2018 Brussels Summit's declaration[7] it is explicitly stated that cyber defence is part of NATO's collective defence.

A major issue in this regard is the difficulty in distinguishing peacetime from crisis or conflict, given the attacker's ability to hide his authorship over the conducted attack – or even the event itself. This is a trait which, unfortunately, is ever-more widespread in an international security environment that features a sort of constant "peacetime war".[8] Against this backdrop, which also saw cyber-attacks multiply during the first wave of COVID-19, in June 2020 the North Atlantic Council stated that all member states are "determined to employ the full range of capabilities, including cyber, to deter, defend against and counter the full spectrum of cyber threats".[9] It is worth noting how NATO declares itself ready to use not only cyber capabilities, but also air, maritime or land capabilities, to counter a cyber-attack. Thus, NATO considers all operational domains in an integrated manner for the purpose of deterrence and defence, in line with the integration of the Cyber Operation Centre in the NATO command structure, as decided during the 2018 Brussels Summit. In order to perform effective deterrence, however, the ability to assign the authorship of attacks is fundamental[10] – a priority which demands further efforts on behalf of the Allies. Concerning the cyber domain, NATO ultimately reaffirms its nature of defensive alliance, as well as the principle for which international law is also applicable to the cyberspace[11] and which has to be

[4] "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack." NATO, *The North Atlantic Treaty*, Washington, 4 April 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm.

[5] NATO, *Remarks by NATO Secretary General Jens Stoltenberg at Cyber Defence Pledge Conference*, London, 23 May 2019, https://www.nato.int/cps/en/natohq/opinions_166039.htm.

[6] NATO, *Deputy Secretary General at CYBERSEC: NATO Is Adapting to Respond to Cyber Threats*, 28 September 2020, https://www.nato.int/cps/en/natohq/news_178338.htm.

[7] NATO, *Brussels Summit Declaration*, 11 July 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

[8] Stefano Silvestri, "Guerre nella globalizzazione: il futuro della sicurezza europea", in *IAI Papers*, No. 20|12 (May 2020), https://www.iai.it/en/node/11674.

[9] NATO, *Statement by the North Atlantic Council concerning Malicious Cyber Activities*, 3 June 2020, https://www.nato.int/cps/en/natohq/official_texts_176136.htm.

[10] Ibid.

[11] For an examination of the main international laws that apply to cyber operations please see: Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge, Cambridge University Press, 2017.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

observed.[12]

The 2019 London Summit gave new politico-strategic impetus to NATO's activities in cyberspace and outer space, in light of the across-the-board geopolitical competition with China and Russia within a global context marked by "aggressive multipolarity".[13] Secretary General Jens Stoltenberg declared that "cyberspace is the new battleground and making NATO cyber ready – well-resourced, well-trained, and well-equipped – is a top priority".[14] Accordingly, the 2020 report of the NATO2030 Reflection Group ascribed great relevance to Emerging and Disruptive Technologies (EDTs), understood both as a sector in which to invest more, and a set of challenges. Within EDTs, those related to cyber defence – above all Artificial Intelligence (AI)[15] – are considered a priority. Indeed, Stoltenberg highlighted that "cyber threats will become more dangerous with the development of new technologies such as AI and machine learning [...]. These technologies are fundamentally changing the nature of warfare, as much as the industrial revolution did. NATO is adapting to this new reality".[16] Hence, the new Strategic Concept, to be presumably defined throughout 2021, will pay great attention to cyber defence, and generally to the cyber domain and EDTs as another field of confrontation with China and Russia.[17]

1.2 NATO structures relevant to cyber defence

Already in 2016, NATO recognised cyberspace as an operational domain, in which the Alliance must be capable of operating as effectively as in the land, maritime and air domains. Such acknowledgement is the starting point for the allied commands to use the cyber domain and resources in their operations and for NATO structures themselves to gear up in this respect.

The Allies maintain their politico-military leadership also in the cyber domain, where NATO structures serve, above all, as support to the decision-making process. For that purpose, the North Atlantic Council is supported by the Cyber Defence Committee, responsible for the political governance of NATO's cyber defence. The Cyber Defence Management Board (CDMB) within the Emerging

[12] NATO, *Statement by the North Atlantic Council concerning Malicious Cyber Activities*, cit.

[13] Alessandro Marrone and Karolina Muti, "NATO's Future: Euro-Atlantic Alliance in a Peacetime War", in *IAI Papers*, No. 20|28 (October 2020), https://www.iai.it/en/node/12251.

[14] Jens Stoltenberg, "NATO Will Defend Itself", in "Cyber Resilience", supplement to *Prospect*, October 2019, p. 6, https://www.prospectmagazine.co.uk/?p=85581.

[15] Thomas de Maizière and A. Wess Mitchell (chairs), *NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General*, 25 November 2020, p. 12, https://www.nato.int/cps/en/natohq/news_179730.htm.

[16] NATO, *Remarks by NATO Secretary General Jens Stoltenberg at Cyber Defence Pledge Conference*, cit.

[17] Alessandro Marrone, "La Nato e la rivalità sistemica con Russia e Cina", in *AffarInternazionali*, 7 December 2020, https://www.affarinternazionali.it/?p=85856.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

Security Challenges Division,[18] gathers in a permanent coordination format the representatives of the military, diplomatic and technical bodies (commands, agencies, etc.), responsible for the various NATO cyber defence activities.

At the operational level, in 2019 a Cyberspace Operations Centre (CYOC) was created within the Allied Command Operations (ACO) in Mons, Belgium. The Centre is responsible for NATO cyber operations, in support of operational commands primarily for monitoring cyberspace and coordinating operations in this domain with those in the land, maritime and air domains.[19] The CYOC could pave the way to the future creation of a NATO command for cyber operations on par with operational commands in the other domains. Beyond the CYOC and its possible evolution, almost all the main elements of NATO integrated military command already have a role to play with regard to cyber defence. As an example, the NATO Force Integration Units (NFIUs) are deployed in the Eastern flank countries to better integrate local forces, from the Baltic to Romania, with those of other member states in order to ensure deterrence and defence vis-à-vis Russia.

At the technical level, the NATO Communications and Information Agency (NCIA), established in 2012, provides many of the capabilities necessary to the Alliance's structures in terms of cyber defence. Moreover, the NCIA directly manages some of the allied networks, interacting with the NATO Cyber Security Centre (NCSC) and the NATO Computer Incident Response Capability (NCIRC). The latter constantly monitors the Alliance's networks, is the first to respond in the event of attacks, files reports on similar instances and provides support to the aforementioned CDMB. Furthermore, the NCIRC, through a specific coordination centre, allows Allies to exchange information and techniques on cyber threats, including some indicators that can provide clues over the nature of occurred attacks.

In 2019 the NCIA renewed for eighteen additional months the contract with defence company Leonardo, in force since 2012, on computer protection services for the Alliance (NCIRC and Cyber Security Support Services – CSSS). A joint staff from Leonardo and NCIA, consisting of about two hundred experts on cyber security, provides NATO personnel in the thirty member countries with services related to detection, management and response to cyber-attacks.[20] In addition, the NATO Cyber Rapid Reaction Teams are available to be promptly employed in support of Allies suffering cyber-attacks.

[18] CCDCOE website: *North Atlantic Treaty Organisation*, https://ccdcoe.org/organisations/nato.

[19] The establishment of CYOC had been set forward by the 2018 Brussels Summit. For further information please see: Alexandra Brzozowski, "NATO Sees New Cyber Command Centre by 2023 as Europe Readies for Cyber Threats", in *Euractiv*, 17 October 2018, https://www.euractiv.com/?p=1281213.

[20] The protection stretches from networks to mobile devices, covering 75 sites, including NATO's headquarters. The service has successfully ensured the cyber security of NATO's 2014, 2016, and 2018 summits. "Cyber security: la NATO estende il contratto con Leonardo", in *Analisi Difesa*, 11 February 2019, https://www.analisidifesa.it/?p=122331.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

Finally, outside the Allied integrated military command, the Cooperative Cyber Defence Centre of Excellence (CCDCOE), inaugurated in Estonia in 2008, prepares studies and reports on issues of interest for cyber defence[21] and, since 2010, hosts periodic exercises. One of such exercises, known as Locked Shield, involved more than one thousand participants in 2019, including institutional leaders and personnel devoted to responding to cyber-attacks, virtually engaged in containing a series of attacks to the critical infrastructures of a country during political elections.[22] Such exercises are very important to prepare civil and military personnel for worst-case cyber-attack scenarios. However, the training should also touch upon people's habits in using electronic devices that weaken NATO's defence capability.[23] The human factor is crucial for cyber defence. In this context, a contribution to allied defence capabilities and resilience is provided by the training courses of the NATO Communications and Information Systems School (NCISS) in Portugal and the NATO school in Oberammergau, Germany, as well as by the research activities on the politico-military level of the NATO Defence College in Rome.

The aforementioned exercises are also important for strengthening cooperation praxis and information exchange. This is the case for the Cyber Coalition Exercise organised by the NATO Allied Command Transformation (ACT), aimed to familiarise the top levels of the decision-making process with a situation of cyber-attack. The information exchange in this sector, however, remains thorny, complicated and politically sensitive, similarly to what happens with intelligence, with possible consequences on the ability to contain and counter the threat. It is crucial to build a trustful relationship within the community of insiders and professionals over time, also on the subsequent use of the shared information. In order to boost information exchange, mutual trust and national capabilities of response to cyber-attacks, since 2015 the CDMB has been tasked with undersigning a Memorandum of Understanding (MoU) on Cyber Defence with the authorities of each member state.[24]

Finally, it is necessary to highlight how, since 2019, member states such as the US, the UK, France, Denmark and Estonia have agreed on a NATO framework within which they are willing to integrate voluntary contributions in terms of defensive and offensive operations.[25] Such capabilities remain, in any case, under the full

[21] See for instance CCDCOE, *Recent Cyber Events and Possible Implications for Armed Forces*, No. 5 (September 2020), https://ccdcoe.org/library/publications/recent-cyber-events-and-possible-implications-for-armed-forces-5.

[22] George Allison, "NATO Takes Part in International Cyber Security Exercise", in *UK Defence Journal*, 11 April 2019, https://ukdefencejournal.org.uk/?p=23095.

[23] Vivienne Machi, "Private Sector Plays Bigger Role in NATO Cyber Strategy", in *National Defence Magazine*, 8 February 2017, https://www.nationaldefensemagazine.org/articles/2017/2/8/private-sector-plays-bigger-role-in-nato-cyber-strategy.

[24] CCDCOE website: *North Atlantic Treaty Organisation*, cit.

[25] Jamie Shea, "Deterring Future Cyberattacks: EU, NATO and International Responses", in "Hybrid and Transnational Threats", in *Friends of Europe Discussion Papers*, Winter 2018, p. 35-38, https://

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

control and responsibility of the country to which they belong.

1.3 The development of military doctrines and capabilities

NATO's recognition of the cyber domain is influencing the development of allied military doctrines and capabilities, as well as the training by member states, so as to enhance their defence and resilience on this front. These are complex, long and laborious processes, necessary to integrate in the military *modus operandi* an operational domain that is new and, in many respects, different from the traditional, physical domains. The CYOC is the key actor in this regard, while the ACT considers the cyber domain in the wider framework of military transformation and technological innovation in a medium-long-term perspective. In the current situation, some allied documents on operational planning already include cyber defence explicitly,[26] but there is still a long way to go to fully incorporate the cyber dimension into NATO's operations and activities, as well as in the doctrinal and capability development, over which member states have the final say.

Allies, for their part, use the Cyber Defence Pledge platform to autonomously evaluate the progresses made over time in the development of national cyber defence capabilities, also through the final report on the implementation of agreed commitments, and to exchange information and good practices in this respect. An important role is also played by the NATO Defence Planning Process (NDPP), the main, all-encompassing and long-term procedure used by member states to agree on national goals for the development of their respective armed forces, so as to also contribute to NATO's collective defence and crisis management commitments. Since 2012, the NDPP includes goals pertaining to the development of cyber defence capabilities, and the related progress is evaluated on a regular basis.

1.4 NATO partnerships with the private sector and the EU

Cooperation between NATO and the industrial counterparts, including those involved in the management of critical infrastructures, is extremely important due to the intrinsic characteristics of the cyber domain, in which technological innovation is mainly driven by private companies that often do not operate in the military field. To this end, in 2014 the Alliance launched the NATO Industry Cyber Partnership (NICP),[27] which envisages, among other things, the participation of industrial representatives in the annual Cyber Defence Workshop, aimed at exchanging highly technical information on threats, vulnerabilities and possible solutions among Allies. The industrial partners, moreover, frequently report to competent NATO structures on the evolution and trends observed in the cyber

www.friendsofeurope.org/insights/hybrid-and-transnational-threats.

[26] See for example: NATO Standardization Office, *Allied Joint Doctrine (AJP-01(E))*, edition E version 1, February 2017, https://www.gov.uk/government/publications/ajp-01-d-allied-joint-doctrine.

[27] NATO Communications and Information (NCI) Agency website: *NATO Industry Cyber Partnership*, https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html.

IAI PAPERS 21 | 05 - FEBRUARY 2021 ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

domain, including the security challenges associated with specific technologies, thus contributing to the allied reflection on this topic.

Cyber defence is listed in the 2016 EU-NATO Joint Declaration[28] among the seven priority areas for the development of bilateral cooperation. On this basis, the institutions of both organisations have exchanged information on strategies, policies, standards and training activities relating to cyber defence, and have taken part in respective trainings – the aforementioned NATO Cyber Coalition, and Cyber Europe on the EU's side. Training is particularly important, with the ambitious plan to jointly train ten thousand staff in the field of cyber defence.[29] In 2016, the two organisations signed a Technical Arrangement on Cyber Defence[30] regulating the exchange of unclassified information, to increase the ability of both organisations to get a more comprehensive situational awareness and to protect the respective networks. NATO-EU cooperation on cyber defence is the subject of regular meetings at the staff level, during which a mutual update occurs also on the respective sectorial activities. The progress made by this partnership was acknowledged by Stoltenberg in 2019.[31]

Beyond the tight cooperation with the EU, NATO is open to cooperating with the United Nations, the Organization for Security and Co-operation in Europe and third states that share the same allied approach to cyber defence. For instance, in 2017 Finland signed the Policy Framework Arrangement with the Alliance, regarding cooperation on cyber defence.[32]

2. The United States

2.1 The Pentagon's strategy: Persistent engagement and forward defence

The US approach to cyber defence is qualitatively and quantitatively different from that of most European countries. Indeed, it is the only world power within NATO, increasingly involved in an all-round geopolitical competition with China – in many respects, almost an equal rival – and with Russia – considered a power in the

[28] European Union and NATO, *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation*, Warsaw, 8 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133163.htm.

[29] NCI Agency, *10,000 Cyber Defenders. Cyber Education for the NATO-EU Workforce*, 29 June 2020, https://www.ncia.nato.int/resources/site1/general/what%20we%20do/nci%20academy/10k_cyber_defender_brochure_20200629.pdf.

[30] Council of the European Union, *EU Cyber Defence Policy Framework (2018 Update)* (14413/18), 19 November 2018, https://www.consilium.europa.eu/media/37024/st14413-en18.pdf.

[31] NATO, *Remarks by NATO Secretary General Jens Stoltenberg at Cyber Defence Pledge Conference*, cit.

[32] NATO, *NATO and Finland Step Up Cyber Defence Cooperation*, 16 February 2017, https://www.nato.int/cps/en/natohq/news_141464.htm.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

position to oppose the US in many sectors. The 2017 National Security Strategy[33] takes note of this geopolitical confrontation and underlines the cyber domain as one of the main battlegrounds. The 2018 National Security Strategy warns against adversarial capabilities to counter and damage American armed forces, economy and society, also in cyberspace.[34]

The US Department of Defence had already established a Cyber Command (USCYBERCOM) in 2009, within the Strategic Command, whose commander wears a double-hat as Director of the National Security Agency (NSA), to ensure synergies between cyber and intelligence operations. Initially, the new Cyber Command only focused on the defence of the Pentagon's networks, but within a few years it became clear that such an approach was inadequate. This is due to the intrinsic characteristics of cyberspace and the fact that it constitutes a major battleground with China and Russia, as well as for the offensive actions conducted by Iran, North Korea and terrorist groups such as the so-called Islamic State of Iraq and Syria (ISIS). The attacks that occurred in 2016 with the hacking of the Democratic Party National Committee's emails, and then those perpetrated in 2017 (WannaCry and NotPetya), have shown adversaries' offensive capabilities deemed unacceptable for American national security.

As a consequence, the current strategic concept of the USCYBERCOM sets out this ambitious goal: "Achieve and maintain superiority in the cyberspace domain to influence adversary behavior, deliver strategic and operational advantages for the Joint Force, and defend and advance our national interests".[35] Such superiority is attained through the "persistence" of operations, maintaining the initiative through an articulated campaign, constantly engaging the adversaries and creating uncertainty over the achievement of their aims. It is fundamentally a seamless campaign of defensive and offensive actions, since the battlefield is interconnected at the global level. In other words, the aim is to operate just up against the adversaries as much as possible, without respite, to deny them an operational advantage whilst creating one for American forces.[36]

In terms of military doctrine, the USCYBERCOM strategy resumes the concept of "forward defence", as explicitly declared by the Secretary of Defence Mark Esper in 2019: a traditional element of the American posture in the land, maritime and air domains, to be put into practice in cyberspace as well.[37] The underlying

[33] White House, *National Security Strategy*, December 2017, https://www.hsdl.org/?abstract&did=806478.

[34] White House, *Summary of the 2018 National Defense Strategy of the United States of America*, January 2018, https://www.hsdl.org/?abstract&did=807329.

[35] US Cyber Command, *Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command*, April 2018, p. 5, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

[36] Ibid., p. 6.

[37] Jim Garamone, "Esper Describes DOD's Increased Cyber Offensive Strategy", in *US Department of Defense News*, 20 September 2019, https://www.defense.gov/Explore/News/Article/Article/1966758.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

assumption, well established by the experience of the first years of activity of the USCYBERCOM, is that limiting cyber defence to responding to cyber-attacks is equivalent to constantly yielding ground to enemies, seeing your own military power eroded, risking the impairment of networks and encouraging hostile powers to deliver increasingly sophisticated attacks. Metaphorically speaking, it is as if the US Navy had remained in American harbours during the Cold War, waiting for Soviet submarines and ships to arrive, instead of patrolling the Atlantic and the Pacific Oceans to ensure sea routes.[38]

Moreover, cyber-attacks against the United States remain regularly under the threshold of armed attack, so to avoid a response from American armed forces which fully mobilises their conventional potential. Due to the impossibility to respond to cyber-attacks outside of cyberspace, the US decided to defend itself by actively and pre-emptively operating against adversaries through USCYBERCOM. Such an approach limits the adversaries' capacity for action, damages their resources, forces them to focus on their own defence and ultimately deters them from certain offensive actions through a credible threat of retaliation.

In this context, the USCYBERCOM strategy is articulated in five imperatives:[39]

1. Achieve and sustain overmatch of adversary capabilities, by anticipating and identifying technological changes and exploiting and operationalising emerging technologies faster and more effectively than the adversaries;
2. Create cyberspace advantages to enhance operations in all domains, by integrating cyberspace capabilities into plans and operations;
3. Create information advantages to support operational outcomes and achieve strategic impact;
4. Operationalise the battlespace for agile and responsive manoeuvre;
5. Expand, deepen, and operationalise partnerships with other American agencies, private sector, allies and academia.

2.2 The evolution of the US Cyber Command

Since 2009, a step change occurred in the United States not only in terms of strategy, but also of mandate and size of the USCYBERCOM. In 2017, the latter was separated from the Strategic Command and raised to a unified command in its own right, on the same level as the land, naval or air counterparts. At the same time, its resources significantly increased: its budget rose from 120 million dollars in 2010 to 600 million in 2018.[40] Two years ago, USCYBERCOM encompassed 133

[38] Paul M. Nakasone, "A Cyber Force for Persistent Operations", in *Joint Force Quarterly*, No. 92 (January 2019), p. 10, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1736950.

[39] US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, cit., p. 8.

[40] Max W.E. Smeets and Herbert Lin, "A Strategic Assessment of the U.S. Cyber Command Vision", in Herbert Lin and Amy Zegart (eds), *Bytes, Bombs, and Spies. The Strategic Dimensions of Offensive Cyber Operations*, Washington, Brookings Institution Press, 2018, p. 81-104, https://link.medium.com/Z4AIqPFEEdb.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

operational groups – double the amount in 2015.[41] The Command is co-located in Fort Meade with the NSA headquarters, in order to ensure maximum synergies with intelligence and homeland security.

The USCYBERCOM's leadership comprises representatives of the cyber commands of the four US armed forces: the Army Cyber Command (ARCYBER), the US Fleet Cyber Command 10th Fleet (FCC/C10F), the US Marine Corps Forces Cyberspace (MARFORCYBER) and the 24th Air Force (AFCYBER) – as well as that of the Coastguard.[42] Among the single armed forces commands, the most experienced is the AFCYBER, established in 2010 and counting 5,400 staff already in 2015.[43] With regard to the personnel, one of the main challenges for USCYBERCOM is hiring and retaining talented computer scientists who could find better career opportunities in the private sector.[44]

Under the new arrangement, the command operates constantly below the threshold of armed attack, whilst prepping to be a "lethal" force in case of conflict.[45] In 2016, USCYBERCOM allegedly destroyed ISIS propaganda material in a server located in Germany.[46] In 2018, it appears that the command disabled the Russian Internet Research Agency's Internet connection.[47] The Agency had long been accused of conducting hacks and interfering in the American electoral process, so the command tried to prevent it from taking action against the US mid-term elections.[48] According to media sources, in 2019 USCYBERCOM placed malware in the software managing Russia's electricity network, responding to an alleged Russian attack against American power grids, in order to exercise a kind of deterrence towards Russian escalation of cyber-attacks.[49] In 2020, an important action by USCYBERCOM against the TrickBot malware, of suspected Russian origin, was officially confirmed for the first time.[50]

41 Ibid.

42 Piret Pernik, Jesse Wojtkowiak and Alexander Verschoor-Kirss, *National Cyber Security Organisation: United States*, Tallinn, CCDCOE, 2016, p. 20, https://www.ccdcoe.org/library/publications/national-cyber-security-organisation-united-states.

43 Ibid., p. 21.

44 Scott Maucione, "What CYBERCOM Is Doing on the Front Lines of Cyberwarfare", in *Federal Insights*, 26 October 2020, https://federalnewsnetwork.com/federal-insights/2020/10/what-cybercom-is-doing-on-the-front-linesof-cyberwarfare.

45 Paul M. Nakasone, "A Cyber Force for Persistent Operations", cit., p. 12.

46 Max Smeets, "NATO Allies Need to Come to Terms with Offensive Cyber Operations", in *Lawfare*, 14 October 2019, https://www.lawfareblog.com/node/17883.

47 Jason Healey, "Taking Down Russian Trolls Is My Kind of Cyber Attack", in *The Cipher Brief*, 28 February 2019, https://www.thecipherbrief.com/?p=30926.

48 David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid", in *The New York Times*, 15 June 2019, https://nyti.ms/2KiTwMl.

49 Ibid.

50 Robert Chesney, "Persisently Engaging TrickBot: USCYBERCOM Takes on a Notorious Botnet", in *Lawfare*, 12 October 2020, https://www.lawfareblog.com/node/19981.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

Against this backdrop, a debate over the cases in which American authorities should be authorised to hit enemies in cyberspace is unfolding[51] and it is not clear if, when and how USCYBERCOM's more aggressive posture has had an impact on adversaries' cyber operations over the past few years.[52]

Finally, it must be noted that former Secretary of Defence Mark Esper repeatedly stressed the importance of US partner countries for an effective American cyber defence vis-à-vis China.[53] Nevertheless, no agreement among NATO countries has yet been reached concerning the procedures and limits of an offensive action within the cyber domain, particularly on access to systems and networks located in another allied country in order to conduct a cyber operation.[54] In this respect, the aforementioned attack carried out by USCYBERCOM against a server in Germany has sparked a certain apprehension within the German government.

3. The United Kingdom

3.1 National strategy

The United Kingdom's approach towards cyber defence operations is very similar to the American one. Since its first Cyber Security Strategy in 2009, London has adopted a centralised approach, at least in elaborating strategies and programmes, and since the subsequent launch of the National Cyber Security Programme it has developed cyber defence capabilities.[55]

In 2013, the UK made public that the development of national capabilities to be employed in the cyber domain included also offensive capabilities. However, the British government's ability to put offensive cyber operations into practice dates back to at least 2007.[56] Also in 2013, the Joint Forces Cyber Group was created: composed of two joint cyber units supported by a Joint Cyber Reserve Force,[57] it operates under the joint guidance of the Ministry of Defence and the Government

[51] Sven Herpig, Robert Morgus and Amit Sheniak, *Active Cyber Defense: A Comparative Study on US, Israeli and German Approaches*, Konrad Adenauer Stiftung, March 2020, p. 9, https://www.kas.de/documents/263458/263507/Active+Cyber+Defense+-+A+comparative+study+on+US,+Israeli+and+German+approaches.pdf.

[52] Mark Pomerleau, "Two Years In, How Has a New Strategy Changed Cyber Operations?", in *Fifth Domain*, 11 November 2019, https://www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations.

[53] Jim Garamone, "Esper Describes DOD's Increased Cyber Offensive Strategy", cit.

[54] Max Smeets, "NATO Allies Need to Come to Terms with Offensive Cyber Operations", cit.

[55] UK Parliament Intelligence and Security Committee (ISC), *Annual Report 2016–2017*, December 2017, p. 35, http://isc.independent.gov.uk/files/2016-2017_ISC_AR.pdf.

[56] Marcus Willett, "Why the UK's National Cyber Force Is an Important Step Forward", in *IISS Analysis*, 20 November 2020, https://www.iiss.org/blogs/analysis/2020/11/uk-national-cyber-force.

[57] UK Strategic Command website: *Working for UKStratCom*, https://www.gov.uk/government/organisations/strategic-command/about/recruitment.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

Communication Headquarters (GCHQ), external to the Ministry of Defence, with the purpose of coordinating all cyber warfare operations.

The 2015 Strategic Defence and Security Review[58] listed cyber threats among the main challenges for the country – and to which the government apparatus must be capable of responding as for any other kind of conventional attack. As a result, in 2016 the National Cyber Security Strategy was issued, centred around three main goals. The first is to ensure the cyber defence and resilience of British networks, as well as of economic activities, private citizens' data and institutions. The second goal is to develop a fast-growing cyber security industry, to ensure the sectorial expertise to develop cutting-edge cyber defence systems. Finally, there is the development of an efficient deterrence capability to make the country a difficult target for attacks. In order to ensure the latter goal, the Strategy outlines the principle of Active Cyber Defence (ACD),[59] i.e., the ability to strengthen the national cyber defence network and system through a constant threat analysis and a consequent update of technological infrastructures.

Furthermore, the possibility to enact offensive cyber operations is foreseen purely for deterrence purposes, meaning also in the absence of an attack,[60] always in compliance with relevant national and international law.[61]

Next, the Strategy lays the groundwork for the creation of the National Cyber Security Centre (NCSC)[62] which, as a central body for cyber security at the national level, plays a prominent role in coordinating sectorial policies. It works with ministries and agencies for the implementation of cyber security programmes. The NCSC benefits from the collaboration with the GCHQ, which – drawing on confidential security information – enables the centre to access full situational awareness, supported by high-level technical expertise.

The NCSC, which envisages to employ 950 experts by the end of 2021,[63] also coordinates the actions of the Cyber Security Operations Centre,[64] i.e., the centre for

[58] UK Government, *National Security Strategy and Strategic Defence and Security Review 2015*, November 2015, https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.

[59] According to the report filed by the National Audit Office, the ACD's goal is among the few objectives that, as of February 2019, had been implemented, up until that moment, without experiencing delays. For further information please see: National Audit Office, *Progress of the 2016–2021 National Cyber Security Programme*, 15 March 2019, p. 30, https://www.nao.org.uk/?p=79229.

[60] Josh Gold, *The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'*, Tallinn, CCDCOE, 2020, p. 14, https://ccdcoe.org/library/publications/the-five-eyes-and-offensive-cyber-capabilities-building-a-cyber-deterrence-initiative.

[61] UK Government, *National Cyber Security Strategy 2016-2021*, November 2016, p. 25, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

[62] Ibid., p. 28-29.

[63] National Audit Office, *Progress of the 2016–2021 National Cyber Security Programme*, cit.

[64] Hemanth Kumar and Talal Husseini, "UK MOD Announced Funding for New Army Cyber Operations Centres", in *Army Technology*, 23 May 2019, https://www.army-technology.com/?p=217317.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

defence and response to cyber-attacks directed against the Ministry of Defence's infrastructures and systems, with the possibility of backup from the armed forces in the event of a highly impacting cyber-attack.

The 2016 National Cyber Security Strategy saw a subsequent allocation of 1.9 billion pounds by the British government throughout the 2016–2021 five-year term, with a 55 per cent increase compared to the previous period, in recognition of the heightened cyber threat.[65] Moreover, the Strategy indicates the launch of two cyber innovation centres, as well as the creation of a fund for defence and cyber innovation of 165 million pounds for the 2016–2021 term, to be employed in innovative and secure-by-design procurement. The Strategy aims to take advantage of the knowledge cumulated within the Cyber Growth Partnership between the government, industry and academia.[66] Such actions seek to attain a full integration of cyber capabilities in current and future military equipment, with the final purpose of integrating cyber defence in terms of planning, organisation, procurement and deployment of the armed forces.[67]

3.2 Offensive cyber operations

As outlined in the Ministry of Defence's Joint Doctrine Note 1/18 on Cyber and Electromagnetic Activities,[68] the defence apparatus includes among offensive cyber operations also deliberate intrusions into the adversary's systems and networks, with the precise purpose of causing damage, destruction or a system malfunctioning. The 2016–2017 Intelligence and Security Committee's Annual Report to Parliament[69] gives an overview of viable offensive operations. These are identified as the ability to:

1. Respond to cyber-attacks;
2. Deny, disrupt or degrade the adversary's communications or weapons systems;
3. Attack wider systems of infrastructure, with the possibility of extending into "real world" damage.

The National Offensive Cyber Programme was tasked with the development of such capabilities already in 2014, thanks to a partnership between the Ministry of Defence and the GCHQ, while possible incidents or intrusion attempts into the Ministry of Defence infrastructure are detected by the MoD Computer Emergency Response Team (MODCERT),[70] which operates within the NCSC.

[65] ISC, *Annual Report 2016–2017*, cit., p. 35.

[66] UK Government, *National Cyber Security Strategy 2016-2021*, cit., p. 58.

[67] UK Ministry of Defence, *Cyber Primer*, 2nd ed., July 2016, https://www.gov.uk/government/publications/cyber-primer.

[68] UK Ministry of Defence, *Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities*, February 2018, https://www.gov.uk/government/publications/cyber-and-electromagnetic-activities-jdn-118.

[69] ISC, *Annual Report 2016–2017*, cit., p. 43.

[70] UK Ministry of Defence, *Cyber Primer*, cit. For an overview of the phases of a cyber-attack response please see p. 55 of the same document.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

The rules of engagement in offensive cyber operations constitute a matter of relevance. At present, indeed, there is no defined and internationally accepted regulatory framework which disciplines how to deploy cyber weapons. In this respect, the United Kingdom also sponsored initiatives such as the Global Conference on Cyberspace, a forum for dialogue between governments, the private sector and civil society to promote the exchange of expertise and discuss the norms at the core of responsible behaviour within cyberspace.[71]

The 2016 Strategy highlights the importance of operating at the international level in contrasting attacks, prompting collaboration also through ad-hoc collaborative frameworks. Notably, together with Australia, Canada, New Zealand and the US, London is part of the Five Eyes Network which represents the closest international partnership as far as intelligence sharing is concerned, and in which the member states commit not to spy on each other and to share detected intelligence signals. London is also part of the successive extensions of the Five Eyes Network, namely the Nine Eyes and the Fourteen Eyes[72] networks, in which the participating states have decreasing access to shared information and, as a consequence, share less of it themselves.[73]

4. France

4.1 Cyber strategy and operational structure

The issue of cyber defence is deemed particularly relevant in France. At the beginning of 2018, former Prime Minister Edouard Philippe entrusted the General Secretariat for Defence and National Security (*Secrétariat General de la Défence et de la Sécurité Nationale*, SGDSN) with the task of drafting a strategy to counter the cyber threat.[74] The document, for inter-ministerial use, provides a clear framework of the cyber risk. It also highlights that, in order to ensure an all-encompassing resilience, it is necessary not only to strengthen the country's technological infrastructures and to possess response capabilities, but also to spread a cyber security culture among the population.[75]

[71] ISC, *Annual Report 2016–2017*, cit., p. 45.

[72] The Nine Eyes Network includes the Five Eyes Network countries plus Denmark, France, the Netherlands and Norway. The Fourteen Eyes Network, finally, also includes Belgium, Germany, Italy, Spain and Sweden.

[73] Sandra Pattison, "Five Eyes, Nine Eyes and Fourteen Eyes: Is Big Brother Watching You?", in *Cloudwards*, 21 May 2020, https://www.cloudwards.net/five-eyes.

[74] SGDSN, *Revue stratégique de cyberdéfense*, 12 February 2018, http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

[75] Ibid., part 1.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

According to the French strategy, known as the Strategic Review of Cyber Defence, cyber deterrence presents three main issues.[76] The first concerns the impossibility of pursuing a clear and credible public stance – that is, to explicitly clarify the modalities and systems through which such dissuasion ought to be conducted. This difficulty stems from the fact that, as opposed to conventional or nuclear deterrence, knowing the modalities of response entails an evolution of attack modes, hence an ineffectiveness of the dissuasion itself. The second limit is linked to the consequences of cyber-attacks, which do not necessarily provoke destructive effects, as is the case with nuclear weapons. Finally, in cyber deterrence it is not possible to ensure international stability in the proliferation of Information Communication Technologies (ICTs) that can be employed for offensive purposes. On the one side, this is due to the fact that these can be used also for non-malicious purposes; on the other side, technologies can be owned also from non-state actors, with the subsequent impossibility of enforcing a certain limit to their proliferation.

From an operational point of view, the 2008 White Paper on Defence laid the groundwork for the establishment of a national agency for the management of cyber-attacks and the protection of the state's information systems, the National Cybersecurity Agency (*Agence nationale de la sécurité des systemes d'information*, ANSSI)[77] within the SGDSN. The creation of the inter-ministerial agency has also determined the distinction between offensive capabilities – information gathering and attack operations – and defensive capabilities – asset protection and defence. As stated in the Strategic Review, this division enables a faster reaction to cyber-attacks and a better coordination with the military cyber defence.[78] Such coordination is ensured by the *Centre de coordination des crises cyber* (C4), which brings together all concerned ministries[79] and makes it possible to implement the most appropriate response in relation to the attack's magnitude. In the event of an offensive cyber event of national relevance or directed towards the armed forces, the Ministry of Defence will directly intervene.[80]

The Agency cooperates with the Cyber Defence Command (*Commandement de la cyberdéfense*, COMCYBER), established in 2017 and responsible for the security and defence of the military systems, infrastructures and operations, with Ministry of Defence support for threat assessment and situational awareness.[81]

[76] Ibid., p. 38.

[77] French Prime Minister, *Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information»*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020828212.

[78] Aude Géry, "La stratégie française de cyberdéfense", in *Brennus 4.0*, March 2020, https://www.penseemiliterre.fr/ressources/30147/14/la_strategie_francaise_de_cyberdefense.pdf.

[79] Amaelle Guiton, "Cyber à la française: l'attaque et la défense, de la «séparation» à l'«interaction»", in *Libération*, 30 January 2020, https://www.liberation.fr/france/2020/01/30/cyber-a-la-francaise-l-attaque-et-la-defense-de-la-separation-a-l-interaction_1776147.

[80] French Senate, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, 11 June 2020, p. 252-255, http://www.senat.fr/rap/r19-506/r19-50638.html.

[81] SGDSN, *Revue stratégique de cyberdéfense*, cit., p. 47.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

The constant technological evolution in the cyber domain, alongside the high number of attacks suffered by the Ministry of Defence,[82] led to the inclusion of a 1.6 billion euro investment in the fight within the cyber domain in the 2019–2025 military programming law (*Loi de programmation militaire*, LPM), as well as an increase in personnel amounting to approximately one thousand "cyber combatants". The staff are to be distributed among the COMCYBER, the *Direction générale de la sécurité extérieure* (DGSE) and the *Direction générale de l'armement* (DGA), to reach a total of 4,500 units in 2025. Of these staff, about half will be dedicated to the protection of information systems, a quarter to cyber defence and the remaining part to offensive cyber operations.[83] Of the total allocation, over the same period of time about 200 million euro will be invested in the construction of the so-called "*temple de la cyberdéfense*" in Saint-Jacques de la Lande, which will host a portion of the one thousand additional cyber experts envisaged by the LPM.[84]
With reference to NATO, the 2018 Strategic Review highlighted the importance of carrying on the work of strengthening allied cyber capabilities through a greater commitment within the Cyber Defence Pledge, together with a better integration of cyber defence capabilities[85] in NATO operational scenarios and missions.[86]

This last concept was further emphasised by Minister of Defence, Florence Parly, who stressed that France will not hesitate to employ cyber weapons in military operations[87] and that cyber combatants, in carrying out their missions, will benefit from the same protections as the soldiers deployed in operations abroad.[88]

4.2 International and industrial sector cooperation

At the regulatory level, France adopted a proactive approach in the search for an internationally shared regulatory framework. For this purpose, in the context of the UN Group of Governmental Experts (GGE), Paris proposed a ban on *hack-*

[82] The Minister of Defence Parly has declared that over the first nine months of 2018 the Ministry had to react to more than 700 cyber-attacks. For further information see: Florence Parly, *Stratégie cyber des Armées*, Paris, 18 January 2019, https://www.defense.gouv.fr/salle-de-presse/discours/discours-de-florence-parly/discour-de-florence-parly-ministre-des-armees-strategie-cyber-des-armees.

[83] Julien Nocetti, "Cyber guerre: la montée des périls", in *Science&Vie*, Spécial Aviation 2019, p. 44-51, https://www.ifri.org/fr/node/16045.

[84] Florence Parly, *Déclaration sur la cyberdéfense*, Rennes, 7 September 2020, https://www.vie-publique.fr/discours/276401-florence-parly-07092020-cyberdefense.

[85] As concerns cyber defence doctrine, France has adopted an approach that is coherent with the inter-Allied one. For an overview of the doctrinal and operational architecture please see: CICDE website: *Sous-domaine 3.20 Cyberdéfense*, https://www.cicde.defense.gouv.fr/images/documentation/architectures/20201222_DOM320.pdf.

[86] SGDSN, *Revue stratégique de cyberdéfense*, cit., p. 92.

[87] Florence Parly, *Déclaration sur la cyberdéfense*, cit.

[88] Florence Parly, *Stratégie cyber des Armées*, cit.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

backs[89] on behalf of private entities and the imposition of checks on the export of cyber components that can be used for malicious purposes. However, the French proposals were not approved because of a lack of consensus among the representatives of the GGE's twenty-five member states.[90] These proposals were an integral part of another French initiative, put forward under the UN aegis and known as the "Paris Call".[91] To ensure a safer use of cyberspace and greater cyber security at the national level, France has requested states' collaboration with private actors, universities and research centres, with the aim of finding a common understanding and reducing possible illicit events.

Moreover, as far as the international context is concerned, France is part of the so-called Fourteen Eyes Agreement, more officially known as SIGINT Seniors Europe. This interstate intelligence sharing agreement links France with thirteen other countries on three continents.[92]

From the industrial standpoint, France has paid great attention to national and European industry development in the cyber domain, so much so that it dedicated part of the 2018 Strategic Review to the partnership between state agencies and private companies in this sector.[93] In November 2019, upon request of Minister Parly, the Ministry of Defence and eight major industries supplying military equipment in France signed a cyber convention that sets out the creation of specific working groups to better meet French needs in terms of cyber defence.[94] More recently, within the action plan for small and medium enterprises (*Action Petites ou moyennes entreprises*, Action PME),[95] the Ministry of Defence promoted the *diagnostic de cyberdéfense* (DIAG Cyber), a system which allows companies to verify their products' cyber resilience and ameliorate their ICT systems thanks to subsidies covering 50 per cent of the costs incurred, for a total of 4.5 million euro for the entire programme.[96]

[89] The term hack-back refers to the whole spectrum of contrast solutions and not only those of infiltration in adversarial ICT systems as response to a cyber-attack.

[90] SGDSN, *Revue stratégique de cyberdéfense*, cit., p. 36.

[91] France Diplomacy, *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

[92] Sven Taylor, "Five Eyes, Nine Eyes, 14 Eyes – Explained", in *Restore Privacy*, September 2020, https://restoreprivacy.com/5-eyes-9-eyes-14-eyes.

[93] French Prime Minister, *Décret n° 2009-834 du 7 juillet 2009*..., cit.

[94] French Ministry of Defence, *Signature d'une convention cyber entre Florence Parly, ministre des Armées, et les industriels de défense*, 15 November 2019, https://www.defense.gouv.fr/english/dga/actualite/signature-d-une-convention-cyber-entre-florence-parly-ministre-des-armees-et-les-industriels-de-defense.

[95] Among others please see: French Ministry of Defence, *Cyberdéfense et innovation: visite de la ministre des armées Florence Parly à Rennes*, 15 October 2019, https://www.defense.gouv.fr/english/dga/actualite/cyberdefense-et-innovation-visite-de-la-ministre-des-armees-florence-parly-a-rennes.

[96] Florence Parly, *Déclaration sur la cyberdéfense*, cit.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

5. Germany

5.1 The Cyber Strategy's operational division and legislative limits

Germany published its first Cyber Security Strategy in 2011, then updated it in 2016 with an inter-ministerial approach[97] that entails action both on behalf of the federal government and at the level of the single Länder administrations. The 2016 Strategy pays particular attention to the necessity of establishing a National Centre for Cyber Response to merge all warnings of potential attacks, and from which to initiate a coordinated response, in line with relevant national and international legislation.

Another innovation introduced in the 2016 Strategy is the mention, for the first time, of the possibility of carrying out offensive cyber operations as retaliation against an attack.[98] It also states that the Military Counterintelligence Service (*Militärische Abschirmdienst*, MAD) is responsible for responding to potential malicious events in the cyber domain. A contribution by the armed forces (*Bundeswehr*) is envisaged, albeit within the general limits set out by the German Constitution, in order to reach the highest levels of operational readiness, possibly through the intervention of incident response teams reporting to the Ministry of Defence.

In Germany, cyber defence is constitutionally entrusted to the *Bundeswehr*, is managed by the Ministry of Defence and has to abide by national and international legislation regulating activities of the armed forces. Given the strong connection between cyber security and defence, the 2016 National Strategy identifies a clear link with the White Book on Defence issued in the same year,[99] and creates a nexus between the cyber defence capabilities of the armed forces and response capabilities within the framework of cyber security. The former are considered as complementary to the build-up of the national cyber security structure, although the two are managed separately. As has occurred in other countries, Germany committed to moving to the joint level infrastructures previously developed at the single branch level, with the purpose of securing a single centre, albeit consisting of separate military operational units.[100] Such a centre is positioned to make use of AI and big data analysis methods in the future, in order to formulate scenarios that

[97] Federal Ministry of the Interior, *Cyber Security Strategy for Germany 2016*, November 2016, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/5f3c65fe954c4d33ad6a9242cd5bb448/file_en.

[98] Sven Herpig, Robert Morgus and Amit Sheniak, *Active Cyber Defense: A Comparative Study on US, Israeli and German Approaches*, cit., p. 4.

[99] Martin Schallbruch and Isabel Marie Skierka, *Cybersecurity in Germany*, Cham, Springer 2018, p. 15-29.

[100] Federal Ministry of the Interior, *Cyber Security Strategy for Germany 2016*, cit., p. 25.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

are as complete as possible.[101]

Given the constant evolution of the cyber domain, already in 2011 Berlin had established a National Council on Cyber Security, which gathers representatives from the Ministries of the Interior, Defence, External Affairs, Economic and Energetic Affairs, Justice and Protection of Consumers, Finance, Education and Research, Transport and Digital Infrastructure as well as representatives of the private sector, with the aim of taking the necessary steps forward towards updating the National Cyber Strategy.[102]

At the operational level, cyber defence in Germany is entrusted to different actors, according to the type of attack and to the goal.

Since 2009, and all the more so following the 2016 European Directive on Network and Information Security (NIS Directive), the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstecknik*, BSI) deals with the operational functioning of cyber defence.[103] In order to do so, the BSI monitors the federal government's networks, investigates security accidents and puts into action the necessary defensive countermeasures. From a military point of view, German armed forces have limited possibilities for collaborating with other state bodies because of the constitutional limits that restrict their support to operations defined as "administrative assistance"[104] – as support to the BSI can be deemed – that are not considered as proper operations. Different is the case of a response to a cyber-attack that, because of its scope[105] and magnitude, demands the deployment of armed forces. In order to be able to operate on the national territory, the military needs parliamentary approval also in the cyber domain, which would take too long in the case of a cyber-attack to allow an effective response. Instead, in the event of cyber defence operations within cooperative frameworks, the initial *Bundestag* approval of the whole mission is sufficient to allow the subsequent use of these cyber defence capabilities.

5.2 Attention to international law and cooperation

Following the publication of the 2016 White Paper, a Cyber and Information Space Command (*Kommando Cyber- und Informationsraum*, CIR) was established. It is tasked with network operations and will comprise as many as 14,000 units of

[101] Ludwig Leinhos, "Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr", in *Connections*, Vol. 19, No. 1 (2020), p. 9-19, https://doi.org/10.11610/Connections.19.1.02.

[102] Federal Ministry of the Interior, *Cyber Security Strategy for Germany 2016*, cit., p. 34.

[103] Federal Office for Information Security: *Cyber-Sicherheit*, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/informationen-und-empfehlungen_node.html.

[104] Martin Schallbruch and Isabel Marie Skierka, *Cybersecurity in Germany*, cit., p. 36.

[105] For the deployment of the *Bundeswehr* on national territory, it is necessary that the attack be carried out by a state actor.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

personnel once full operational capacity is reached, as planned, in 2021.[106] The Command is in charge of intervening in cases of direct attack against armed forces or government facilities, perpetrated by another country. However, considering the peculiarity of the cyber threat, it is not always possible to identify the attacker at once, thus creating the necessity of coordinating the different authorities involved in the response[107] and better regulating the potential cooperation of armed forces.[108] With this in mind, already in 2011 the federal government had established the National Centre for Cyber Defence (*Cyber-Abwehrzentrum*, Cyber-AZ), mandated exclusively with the task of coordinating the different entities.[109]

In its national strategies on cyberspace, Germany has always highlighted the necessity of operating within regulatory frameworks that are as complete as possible, and through the formation of partnerships to reach higher levels of security and operational readiness, also in the case of retaliation against cyber-attacks.[110] From a legal standpoint, in the present state active defence operations are not explicitly regulated and a debate on the opportunity to envisage *hack-backs* is ongoing at the national level.[111] In the international sphere, Germany is a member of the GGE[112] as well as the Fourteen Eyes Network.

Another aspect closely considered by the German government is cooperation with the private sector so as to guarantee that the country has systems and infrastructures that are as advanced as possible. In 2018, the Ministries of Defence and Interior envisaged the establishment of an Agency of Innovation in cyber security, with the mandate to sign contracts for research projects with a great technological potential.[113] The Agency was only established in August 2020 and will receive an overall funding of 350 million euro until 2023.[114]

[106] Alessandro Rugolo, "Anche la Germania ha la sua quarta forza armata", in *Difesa Online*, 16 July 2018, https://www.difesaonline.it/node/10773.

[107] Martin Schallbruch and Isabel Marie Skierka, *Cybersecurity in Germany*, cit., p. 37.

[108] Matthias Schulze, "German Military Cyber Operations are in a Legal Gray Zone", in *Lawfare*, 8 April 2020, https://www.lawfareblog.com/node/18950.

[109] Martin Schallbruch and Isabel Marie Skierka, *Cybersecurity in Germany*, cit., p. 39.

[110] Federal Ministry of the Interior, *Cyber Security Strategy for Germany 2016*, cit., p. 21.

[111] Matthias Becker, "Der geheime Krieg im Netz", in *Deutschlandfunk*, 16 October 2020, https://www.deutschlandfunk.de/aktive-cyber-abwehr-fuer-deutschland-der-geheime-kriegim.724.de.html?dram:article_id=461140.

[112] The GGE comprises 25 representatives from as many states. For further information on the composition and tasks see: United Nations Office for Disarmament Affairs (UNODA) website: *Group of Governmental Experts*, https://www.un.org/disarmament/group-of-governmental-experts.

[113] Ludwig Leinhos, "Cyber Defence in Germany", cit.

[114] "Germany Launches Cybersecurity Agency to Strengthen 'Digital Sovereignty'", in *Deutsche Welle*, 11 August 2020, https://p.dw.com/p/3gnWA.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

6. Spain

6.1 Strategic update and the restructuring of the armed forces

According to certain statistics, Spain is among those European countries where the highest numbers of attacks in the cyber domain have been recorded.[115] While some of these attacks are directed towards nonstrategic sectors, others correspond to a kind of cyber espionage with severe consequences, as in the case of the prolonged attack perpetrated against the Spanish Ministry of Defence in 2019, for the purpose of gathering sensitive industrial information.[116]

Spain's National Strategy for Cyber Security was updated in 2019[117] in order to take into account the instructions set out by the 2017 National Security Strategy. Nonetheless, because of COVID-19 the necessity to update the strategic document again in 2021 has been highlighted, so as to consider the possible consequences on the cyber domain of prolonged pandemics. For that matter, massive recourse to working from home and an increased use of online platforms make it necessary to upgrade the systems and strategies designed to counter cyber-attacks and to make technological structures more resilient, also by including better training for personnel and users, as put forward by the EU Security Union Strategy.[118]

In the meantime, in May 2020 the Royal Decree No. 521/2020[119] on the core organisation of the armed forces was issued. The document lays great emphasis on the necessity of having adequately trained and technologically advanced staff, structures and defence systems, so as to allow the digital transformation of the Spanish armed forces, also considering the increased cyber threat.

As in other NATO countries, cyber defence is part of the wider framework of cyber security, which includes – but is not limited to – activities linked to the armed forces. This approach was further expanded with the June 2020 Directive on National Defence, which stated that the current international security environment, as well as emerging threats, make essential a better and closer collaboration of the armed forces with the national security system, in order to

[115] EnigmaSoft, *Top 20 Countries Found to Have the Most Cybercrime*, updated 21 April 2017, https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime.

[116] Miguel González, "Una 'potencia extranjera' atacó los ordenadores de Defensa", in *El País*, 27 March 2019, https://elpais.com/politica/2019/03/25/actualidad/1553543912_758690.html.

[117] National Cryptologic Centre (CCN), *Spanish Approach to Cybersecurity. Decalogue CCN-CERT*, June 2019, p. 8, https://www.ccn.cni.es/index.php/en/menu-ccn-en/spanish-approach-to-cybersecurity.

[118] European Commission, *Communication on the EU Security Union Strategy* (COM/2020/605), 24 July 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605.

[119] Spanish Ministry of Defence, *Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas*, 21 May 2020, https://www.boe.es/eli/es/rd/2020/05/19/521/con.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

ensure the protection of citizens and the state within an integrated framework.[120] In the cyber field, already in 2008 Spain had equipped itself with two centres of response to cyber-attacks: the Spanish National Cybersecurity Institute (*Instituto Nacional de Ciberseguridad*) Computer Emergency Response Team (INCIBE-CERT) and the National Cryptologic Centre (*Centro Criptológico Nacional*) Computer Emergency Response Team (CCN-CERT). Whilst the former is a rapid response team for cyber-attacks directed against citizens, businesses and other relevant actors, the latter focuses on the response to attacks perpetrated against governmental institutions.[121] In the military sphere, the Cyber Defence Joint Command (*Mando Conjunto de Ciberdefensa*, MCCD),[122] directly subordinated to the Spanish Defence Staff, is responsible for executing actions linked to the cyber defence of ICT infrastructures and systems of the Spanish defence apparatus. The MCCD is notably mandated with enacting operations that are necessary to ensure the cyber integrity of such structures and of military capabilities, including cyber systems. Established by Ministerial Decree No. 10/2013,[123] the Command is also responsible for contributing to the appropriate response in the event of a cyber-attack against the nation. Given the extent of the cyber domain, the MCCD's actions must follow operational guidelines that take into account the so-called list of cyber priority assets, by defining the type of response and prioritisation of such assets to be protected, according to the magnitude of the potential damage caused by a cyber-attack.[124] The Spanish Ministry of Defence is also equipped with a computer emergencies response team for incidents occurring in the military sector (ESPCERTDEF), which cooperates with the other national, civil CERTs.[125]

Since the Joint Command is subordinated to the Defence Staff, it is plausible to assume that cyber operations – defensive or not – could be integrated within the chain of command also in cases of multinational deployments of the armed forces, be it under the aegis of NATO, the EU or the UN. Nevertheless, in the absence of a declared armed conflict, the possibility of conducting offensive operations is not envisaged at the moment – as opposed to what happens for instance in the UK.[126]

[120] Spanish Government, *Directiva de Defensa Nacional 2020*, 11 June 2020, https://www.dsn.gob.es/es/node/12548.

[121] Bernard Meyer, "Cybersecurity in Spain", in *CyberNews*, 6 November 2019, https://cybernews.com/?p=410.

[122] Spanish Ministry of Defence, *Real Decreto 521/2020*, cit., article 13.

[123] Spanish Ministry of Defence, "Orden Ministerial 10/2013, de 19 de febrero", in *Colección Legislativa del Ministerio de Defensa. Año 2013*, 2014, p. 102-103, https://publicaciones.defensa.gob.es/coleccion-legislativa-del-ministerio-de-defensa-a-o-2013.html.

[124] Javier López de Turiso y Sánchez, *Concepto de las Operationes en el Cyberespacio, presentation at the III Cyber Defence Symposium of the Spanish Joint Cyber Defence Command*, Madrid, 25 May 2016, p. 17-18, https://jornadasciberdefensa.es/2016/programa/59/en.

[125] CCN, *Spanish Approach to Cybersecurity*, cit., p. 13 and 19.

[126] Centro Superior de Estudios de la Defensa Nacional (CESEDEN), "El ciberespacio. Nuevo escenario de confrontación", in *Monografías del CESEDEN*, No. 126 (February 2012), p. 52, https://dialnet.unirioja.es/servlet/libro?codigo=547632.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

6.2 Industrial cooperation and training

Spain's cyber security strategy pays particular attention to international cooperation, as well as awareness on the part of citizens and officials regarding the correct use of cyberspace. With reference to the first point, at the European level Spain is leading projects within the European Defence Industrial Development Programme (EDIDP) contributing to higher levels of cyber security. Among these, Madrid coordinates enterprises and research centres in four countries[127] as part of the European Cyber Situational Awareness Platform (ECYSAP), which aims to provide an integrated picture of potential cyber threats that can target defence systems to enable the armed forces to respond promptly, also thanks to the support of decision-making tools.[128]

From an educational perspective, on the other hand, the strategy focuses particularly on the necessity of providing operators – be they civil or military – with specialised training. The Spanish training plan is entrusted to the National Cryptologic Centre (CCN), but specific activities can also take place through dedicated partnerships, such as the one undertaken between the Ministry of Defence and the National Institute of Cybersecurity (INCIBE) in 2020. The agreement envisages that training courses will be offered to young students, with the aim of creating more employment opportunities for national talent in Spain's cyber defence.[129]

Conclusions

The cyber threat

In the last two decades, the number of cyber-attacks has increased considerably, to the extent of becoming a proper threat to national security and the defence of the state. In order to mitigate the occurrence of such attacks, numerous initiatives have been put forward at the international level with the aim of regulating legal actions within cyberspace. These initiatives, however, have produced limited results due to divergences concerning the use of the cyber domain, above all by states such as Russia and China.

[127] European Commission, *ECYSAP. European Cyber Situational Awareness Platform*, June 2020, https://ec.europa.eu/commission/presscorner/api/files/attachment/865731/EDIDP%20-%20ECYSAP.pdf.pdf.

[128] Spanish Government, *Leon's Proposal. Spanish Proposal to host the European Cybersecurity Industrial, Technology and Research Competence Centre*, November 2020, p. 106, https://www.consilium.europa.eu/media/46697/spanish-proposal-to-host-the-european-cybersecurity-industrial-technology-and-research-competence-centre.pdf.

[129] Alfonso de Castañeda, "Defensa capacitará a 200 militares españoles en materia de ciberseguridad", in *Zona Movilidad*, 6 March 2020, https://www.zonamovilidad.es/mvc/amp/noticia/23439.

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

The lack of regulations is amplified by two additional factors. Firstly, whereas a conventional attack can be perpetrated by states or terrorist groups, a cyber-attack can be carried out by a wider pool of actors, thus increasing the likelihood of such occurrence, usually with poorly identifiable authorship. Secondly, the fast-paced technological innovation in this field demands constant attention to, and investment in, defensive technologies. This in turns implicates the employment of highly specialised technical personnel, which is not sufficient in the public sectors of the countries covered by this study – also considering the appeal of the private sector.

The allied response

The potential pervasiveness of cyber-attacks led NATO to declare cyberspace a domain of operation in 2016, *de facto* taking a step change in its approach toward this kind of threat. These attacks can also trigger the collective defence clause pursuant to article 5 of the North Atlantic Treaty, in recognition of the fact that the cyber element will increasingly be embedded in conventional conflicts. Currently, cyber defence is a support element of land, air and sea operational commands, but the possibility of the future creation of a NATO command for cyber operations remains open, following the formulation of doctrines and capability development – a process currently in its early stages. Meanwhile, NATO's NCSC and the NCIRC provide support through constant monitoring and assistance with response to a cyber-attack event, also putting the Cyber Reaction Teams at the disposal of member countries.

Cyber defence at the NATO level is not limited to the creation of command structures and the employment of dedicated personnel, but also involves partnerships with different actors. The necessity of equipping the Atlantic Alliance with cutting-edge technology led in 2014 to the formation of specific partnerships with industries operating in the cyber sector. NATO-EU cooperation was already listing the cyber dimension among priority areas of collaboration in 2016.

National necessities

The analysis of five national case studies has resulted in the identification of different approaches towards cyber defence, as proof of how much has yet to be accomplished in defining shared doctrines and procedures. Among the countries taken into consideration, a substantial divide can be traced between states that envisage the possibility of carrying out exclusively defensive actions, and those that count on the ability to perform offensive operations also in the absence of a cyber-attack.

Among the first group are Germany and Spain, which envision cyber deterrence as the country's ability to promptly and adequately respond to a cyber-attack, enacting what is defined as *hack-back*. Additional differences between Berlin and Madrid concern the possibility of deploying the armed forces on national territory

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

in the event of an attack, which would need prior authorisation by Parliament in Germany. It is important to note, however, that this procedure poorly matches the speed of reaction necessary to limit or avoid the damage of a cyber-attack: parliamentary timeframes, in cases that require rapid and tailored actions, could mean the state's inability to protect its primary interests and thus hinder national defence.

London, Paris and Washington, by contrast, have a different understanding of the possibilities deriving from an active use of cyber defence. For the three capitals, cyber defence and deterrence are about ensuring not only reaction capabilities in the event of a cyber-attack, but also the possibility of a preventive action against potential adversaries, be they state or non-state actors. Following this logic, for instance, the UK carried out a cyber-attack to the detriment of ISIS in 2016.

Despite these differences, it is possible to outline shared necessities among the five countries taken into consideration, which can be summed up as follows:

- Necessity to have a shared regulatory and doctrinal framework at the NATO, EU and international level;
- Better integration of the cyber element in national and allied command structures;
- More structured and strategic collaboration with enterprises and research entities;
- Specialised training of military personnel devoted to protection from the cyber threat; and
- Increased awareness about the use of cyberspace among state officials, critical infrastructure managers and the population in general.

Updated 5 February 2021

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

References

George Allison, "NATO Takes Part in International Cyber Security Exercise", in *UK Defence Journal*, 11 April 2019, https://ukdefencejournal.org.uk/?p=23095

Matthias Becker, "Der geheime Krieg im Netz", in *Deutschlandfunk*, 16 October 2020, https://www.deutschlandfunk.de/aktive-cyber-abwehr-fuer-deutschland-der-geheime-kriegim.724.de.html?dram:article_id=461140

Alexandra Brzozowski, "NATO Sees New Cyber Command Centre by 2023 as Europe Readies for Cyber Threats", in *Euractiv*, 17 October 2018, https://www.euractiv.com/?p=1281213

Centro Superior de Estudios de la Defensa Nacional (CESEDEN), "El ciberespacio. Nuevo escenario de confrontación", in *Monografías del CESEDEN*, No. 126 (February 2012), p. 52, https://dialnet.unirioja.es/servlet/libro?codigo=547632

Robert Chesney, "Persisently Engaging TrickBot: USCYBERCOM Takes on a Notorious Botnet", in *Lawfare*, 12 October 2020, https://www.lawfareblog.com/node/19981

Alfonso de Castañeda, "Defensa capacitará a 200 militares españoles en materia de ciberseguridad", in *Zona Movilidad*, 6 March 2020, https://www.zonamovilidad.es/mvc/amp/noticia/23439

Thomas de Maizière and A. Wess Mitchell (chairs), *NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General*, 25 November 2020, https://www.nato.int/cps/en/natohq/news_179730.htm

Cooperative Cyber Defence Centre of Excellence (CCDCOE), *Recent Cyber Events and Possible Implications for Armed Forces*, No. 5 (September 2020), https://ccdcoe.org/library/publications/recent-cyber-events-and-possible-implications-for-armed-forces-5

Council of the European Union, *EU Cyber Defence Policy Framework (2018 Update)* (14413/18), 19 November 2018, https://www.consilium.europa.eu/media/37024/st14413-en18.pdf

European Commission, *Communication on the EU Security Union Strategy* (COM/2020/605), 24 July 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605

European Commission, *ECYSAP. European Cyber Situational Awareness Platform*, June 2020, https://ec.europa.eu/commission/presscorner/api/files/attachment/865731/EDIDP%20-%20ECYSAP.pdf.pdf

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

European Union and NATO, *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation*, Warsaw, 8 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133163.htm

Federal Ministry of the Interior, *Cyber Security Strategy for Germany 2016*, November 2016, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/5f3c65fe954c4d33ad6a9242cd5bb448/file_en

France Diplomacy, *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

French General Secretariat for Defence and National Security, *Revue stratégique de cyberdéfense*, 12 February 2018, http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

French Ministry of Defence, *Cyberdéfense et innovation: visite de la ministre des armées Florence Parly à Rennes*, 15 October 2019, https://www.defense.gouv.fr/english/dga/actualite/cyberdefense-et-innovation-visite-de-la-ministre-des-armees-florence-parly-a-rennes

French Ministry of Defence, *Signature d'une convention cyber entre Florence Parly, ministre des Armées, et les industriels de défense*, 15 November 2019, https://www.defense.gouv.fr/english/dga/actualite/signature-d-une-convention-cyber-entre-florence-parly-ministre-des-armees-et-les-industriels-de-defense

French Prime Minister, *Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information»*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020828212

French Senate, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2019-2020*, 11 June 2020, http://www.senat.fr/rap/r19-506/r19-50638.html

Jim Garamone, "Esper Describes DOD's Increased Cyber Offensive Strategy", in *US Department of Defense News*, 20 September 2019, https://www.defense.gov/Explore/News/Article/Article/1966758

Aude Géry, "La stratégie française de cyberdéfense", in *Brennus 4.0*, March 2020, https://www.penseemiliterre.fr/ressources/30147/14/la_strategie_francaise_de_cyberdefense.pdf

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

Josh Gold, *The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'*, Tallinn, CCDCOE, 2020, https://ccdcoe.org/library/publications/the-five-eyes-and-offensive-cyber-capabilities-building-a-cyber-deterrence-initiative

Miguel González, "Una 'potencia extranjera' atacó los ordenadores de Defensa", in *El País*, 27 March 2019, https://elpais.com/politica/2019/03/25/actualidad/1553543912_758690.html

Amaelle Guiton, "Cyber à la française: l'attaque et la défense, de la «séparation» à l'«interaction»", in *Libération*, 30 January 2020, https://www.liberation.fr/france/2020/01/30/cyber-a-la-francaise-l-attaque-et-la-defense-de-la-separation-a-l-interaction_1776147

Jason Healey, "Taking Down Russian Trolls Is My Kind of Cyber Attack", in *The Cipher Brief*, 28 February 2019, https://www.thecipherbrief.com/?p=30926

Sven Herpig, Robert Morgus and Amit Sheniak, *Active Cyber Defense: A Comparative Study on US, Israeli and German Approaches*, Konrad Adenauer Stiftung, March 2020, https://www.kas.de/documents/263458/263507/Active+Cyber+Defense+-+A+comparative+study+on+US,+Israeli+and+German+approaches.pdf

Hemanth Kumar and Talal Husseini, "UK MOD Announced Funding for New Army Cyber Operations Centres", in *Army Technology*, 23 May 2019, https://www.army-technology.com/?p=217317

Ludwig Leinhos, "Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr", in *Connections*, Vol. 19, No. 1 (2020), p. 9-19, https://doi.org/10.11610/Connections.19.1.02

Javier López de Turiso y Sánchez, *Concepto de las Operationes en el Cyberespacio*, presentation at the III Cyber Defence Symposium of the Spanish Joint Cyber Defence Command, Madrid, 25 May 2016, p. 17-18, https://jornadasciberdefensa.es/2016/programa/59/en

Vivienne Machi, "Private Sector Plays Bigger Role in NATO Cyber Strategy", in *National Defence Magazine*, 8 February 2017, https://www.nationaldefensemagazine.org/articles/2017/2/8/private-sector-plays-bigger-role-in-nato-cyber-strategy

Alessandro Marrone, "La Nato e la rivalità sistemica con Russia e Cina", in *AffarInternazionali*, 7 December 2020, https://www.affarinternazionali.it/?p=85856

Alessandro Marrone and Karolina Muti, "NATO's Future: Euro-Atlantic Alliance in a Peacetime War", in *IAI Papers*, No. 20|28 (October 2020), https://www.iai.it/en/node/12251

Scott Maucione, "What CYBERCOM Is Doing on the Front Lines of Cyberwarfare", in *Federal Insights*, 26 October 2020, https://federalnewsnetwork.com/federal-

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

insights/2020/10/what-cybercom-is-doing-on-the-front-linesof-cyberwarfare

Stefano Mele, "La strategia della Nato in ambito cyber", in *Europa Atlantica*, 3 June 2019, https://wp.me/pabS04-e4

Bernard Meyer, "Cybersecurity in Spain", in *CyberNews*, 6 November 2019, https://cybernews.com/?p=410

Paul M. Nakasone, "A Cyber Force for Persistent Operations", in *Joint Force Quarterly*, No. 92 (January 2019), p. 10-14, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1736950

National Audit Office, *Progress of the 2016–2021 National Cyber Security Programme*, 15 March 2019, https://www.nao.org.uk/?p=79229

National Cryptologic Centre (CCN), *Spanish Approach to Cybersecurity. Decalogue CCN-CERT*, June 2019, https://www.ccn.cni.es/index.php/en/menu-ccn-en/spanish-approach-to-cybersecurity

NATO, *Brussels Summit Declaration*, 11 July 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm

NATO, *Cyber Defence Pledge*, 8 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO, *Deputy Secretary General at CYBERSEC: NATO Is Adapting to Respond to Cyber Threats*, 28 September 2020, https://www.nato.int/cps/en/natohq/news_178338.htm

NATO, *NATO and Finland Step Up Cyber Defence Cooperation*, 16 February 2017, https://www.nato.int/cps/en/natohq/news_141464.htm

NATO, *The North Atlantic Treaty*, Washington, 4 April 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm

NATO, *Remarks by NATO Secretary General Jens Stoltenberg at Cyber Defence Pledge Conference*, London, 23 May 2019, https://www.nato.int/cps/en/natohq/opinions_166039.htm

NATO, *Statement by the North Atlantic Council concerning Malicious Cyber Activities*, 3 June 2020, https://www.nato.int/cps/en/natohq/official_texts_176136.htm

NATO, *Strategic Concept 2010*, 19 November 2010, https://www.nato.int/cps/en/natohq/topics_82705.htm

NATO Communications and Information Agency, *10,000 Cyber Defenders. Cyber Education for the NATO-EU Workforce*, 29 June 2020, https://www.ncia.nato.int/

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

resources/site1/general/what%20we%20do/nci%20academy/10k_cyber_defender_brochure_20200629.pdf

NATO Standardization Office, *Allied Joint Doctrine (AJP-01(E))*, edition E version 1, February 2017, https://www.gov.uk/government/publications/ajp-01-d-allied-joint-doctrine

Julien Nocetti, "Cyber guerre: la montée des périls", in *Science&Vie*, Spécial Aviation 2019, p. 44-51, https://www.ifri.org/fr/node/16045

Florence Parly, *Déclaration sur la cyberdéfense*, Rennes, 7 September 2020, https://www.vie-publique.fr/discours/276401-florence-parly-07092020-cyberdefense

Florence Parly, *Stratégie cyber des Armées*, Paris, 18 January 2019, https://www.defense.gouv.fr/salle-de-presse/discours/discours-de-florence-parly/discour-de-florence-parly-ministre-des-armees-strategie-cyber-des-armees

Sandra Pattison, "Five Eyes, Nine Eyes and Fourteen Eyes: Is Big Brother Watching You?", in *Cloudwards*, 21 May 2020, https://www.cloudwards.net/five-eyes

Piret Pernik, Jesse Wojtkowiak and Alexander Verschoor-Kirss, *National Cyber Security Organisation: United States*, Tallinn, CCDCOE, 2016, https://www.ccdcoe.org/library/publications/national-cyber-security-organisation-united-states

Mark Pomerleau, "Two Years In, How Has a New Strategy Changed Cyber Operations?", in *Fifth Domain*, 11 November 2019, https://www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations

Alessandro Rugolo, "Anche la Germania ha la sua quarta forza armata", in *Difesa Online*, 16 July 2018, https://www.difesaonline.it/node/10773

David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid", in *The New York Times*, 15 June 2019, https://nyti.ms/2KiTwMl

Martin Schallbruch and Isabel Marie Skierka, *Cybersecurity in Germany*, Cham, Springer 2018

Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge, Cambridge University Press, 2017

Matthias Schulze, "German Military Cyber Operations are in a Legal Gray Zone", in *Lawfare*, 8 April 2020, https://www.lawfareblog.com/node/18950

Jamie Shea, "Deterring Future Cyberattacks: EU, NATO and International Responses", in "Hybrid and Transnational Threats", in *Friends of Europe Discussion Papers*, Winter 2018, p. 35-38, https://www.friendsofeurope.org/insights/hybrid-

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

and-transnational-threats

Stefano Silvestri, "Guerre nella globalizzazione: il futuro della sicurezza europea", in *IAI Papers*, No. 20|12 (May 2020), https://www.iai.it/en/node/11674

Max Smeets, "NATO Allies Need to Come to Terms with Offensive Cyber Operations", in *Lawfare*, 14 October 2019, https://www.lawfareblog.com/node/17883

Max W.E. Smeets and Herbert Lin, "A Strategic Assessment of the U.S. Cyber Command Vision", in Herbert Lin and Amy Zegart (eds), *Bytes, Bombs, and Spies. The Strategic Dimensions of Offensive Cyber Operations*, Washington, Brookings Institution Press, 2018, p. 81-104, https://link.medium.com/Z4AIqPFEEdb

Spanish Government, *Directiva de Defensa Nacional 2020*, 11 June 2020, https://www.dsn.gob.es/es/node/12548

Spanish Government, *Leon's Proposal. Spanish Proposal to host the European Cybersecurity Industrial, Technology and Research Competence Centre*, November 2020, https://www.consilium.europa.eu/media/46697/spanish-proposal-to-host-the-european-cybersecurity-industrial-technology-and-research-competence-centre.pdf

Spanish Ministry of Defence, "Orden Ministerial 10/2013, de 19 de febrero", in *Colección Legislativa del Ministerio de Defensa. Año 2013*, 2014, p. 102-103, https://publicaciones.defensa.gob.es/coleccion-legislativa-del-ministerio-de-defensa-a-o-2013.html

Spanish Ministry of Defence, *Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas*, 21 May 2020, https://www.boe.es/eli/es/rd/2020/05/19/521/con

Jens Stoltenberg, "NATO Will Defend Itself", in "Cyber Resilience", supplement to *Prospect*, October 2019, p. 4-6, https://www.prospectmagazine.co.uk/?p=85581

Sven Taylor, "Five Eyes, Nine Eyes, 14 Eyes – Explained", in *Restore Privacy*, September 2020, https://restoreprivacy.com/5-eyes-9-eyes-14-eyes

UK Government, *National Cyber Security Strategy 2016-2021*, November 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

UK Government, *National Security Strategy and Strategic Defence and Security Review 2015*, November 2015, https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015

UK Ministry of Defence, *Cyber Primer*, 2nd ed., July 2016, https://www.gov.uk/government/publications/cyber-primer

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

UK Ministry of Defence, *Joint Doctrine Note 1/18: Cyber and Electromagnetic Activities*, February 2018, https://www.gov.uk/government/publications/cyber-and-electromagnetic-activities-jdn-118

UK Parliament Intelligence and Security Committee (ISC), *Annual Report 2016–2017*, December 2017, http://isc.independent.gov.uk/files/2016-2017_ISC_AR.pdf

US Cyber Command, *Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command*, April 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf

White House, *National Security Strategy*, December 2017, https://www.hsdl.org/?abstract&did=806478

White House, *Summary of the 2018 National Defense Strategy of the United States of America*, January 2018, https://www.hsdl.org/?abstract&did=807329

Marcus Willett, "Why the UK's National Cyber Force Is an Important Step Forward", in *IISS Analysis*, 20 November 2020, https://www.iiss.org/blogs/analysis/2020/11/uk-national-cyber-force

List of interviewees

Felix Arteaga, Senior Researcher, Real Instituto Elcano

Guillem Colom-Piella, Director of Studies of the Political and Administrative Sciences Department, Universidad Pablo de Olavide

Enrique Fojon, Colonel and doctor in International Relations, former Head of Unit for transformation of the Armed Forces and advisor to the Spanish Ministry of Defence

Bastian Giegerich, Defence and Military Analysis Director, International Institute for Strategic Studies (IISS)

Claudia Major, International Security Research Division Director, Stiftung Wissenschaft und Politik (SWP)

Jean-Pierre Maulny, Deputy Director, Institut de Relations Internationales et Stratégiques (IRIS)

Neil Robinson, Policy Officer, NATO Cyber Defence Emerging and Security Division

Max William Smeets, Director, European Cyber Conflict Research Initiative (ECCRI)

Göran Swistek, Military Officer, International Security Research Division, Stiftung Wissenschaft und Politik (SWP)

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

List of acronyms

ACD	Active Cyber Defence
ACO	Allied Command Operations (NATO)
ACT	Allied Command Transformation (NATO)
Action PME	Action Petites ou moyennes entreprises
AFCYBER	24th Air Force (US)
AI	Artificial Intelligence
ANSSI	Agence nationale de la sécurité des systèmes d'information
ARCYBER	Army Cyber Command (US)
BSI	Bundesamt für Sicherheit in der Informationstecknik
C4	Centre de coordination des crises cyber
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CCN	Centro Criptológico Nacional
CDMB	Cyber Defence Management Board (NATO)
CERT	Computer Emergency Response Team
CIR	Cyber- und Informationsraum
COMCYBER	Commandement de la cyberdéfense
CSSS	Cyber Security Support Services (NATO)
Cyber-AZ	Cyber-Abwehrzentrum
CYOC	Cyberspace Operations Centre (NATO)
DGA	Direction générale de l'armement
DGSE	Direction générale de la sécurité extérieure
DIAG Cyber	Diagnostic de cyberdéfense
ECYSAP	European Cyber Situational Awareness Platform
EDIDP	European Defence Industrial Development Programme
EDT	Emerging and Disruptive Technology
ESPCERTDEF	Computer Emergency Response Team in the field of the Ministry of Defence (Spain)
FCC/C10F	Fleet Cyber Command 10th Fleet (US)
GCHQ	Government Communication Headquarters
GGE	Group of Governmental Experts (UN)
ICT	Information Communication Technology
INCIBE	Instituto Nacional de Ciberseguridad
ISIS	Islamic State of Iraq and Syria
LPM	Loi de programmation militaire
MAD	Militärische Abschirmdienst
MARFORCYBER	Marine Corps Forces Cyberspace (US)
MCCD	Mando Conjunto de Cyberdefensa
MODCERT	Ministry of Defence Computer Emergency Response Team

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

MoU	Memorandum of Understanding
NCIA	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability
NCISS	NATO Communications and Information Systems School
NCSC	NATO Cyber Security Centre
NDPP	NATO Defence Planning Process
NFIU	NATO Force Integration Unit
NICP	NATO Industry Cyber Partnership
NIS	Network and Information Security
NSA	National Security Agency
SGDSN	Secrétariat général de la défense et de la sécurité nationale
USCYBERCOM	US Cyber Command

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI

Istituto Affari Internazionali (IAI)
The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*Affarinternazionali*), three book series (*Global Politics and Security*, *Quaderni IAI* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via dei Montecatini, 17 - I-00186 Rome, Italy
T +39 06 697683
iai@iai.it
www.iai.it

Latest IAI PAPERS

Director: Riccardo Alcaro (r.alcaro@iai.it)

21 | 05 Alessandro Marrone and Ester Sabatino, *Cyber Defence in NATO Countries: Comparing Models*
21 | 04 Katarzyna Kubiak, *Reviewing NATO's Non-proliferation and Disarmament Policy*
21 | 03 Mehdi Lahlou, *EU–Africa Partnership on Migration and Mobility in Light of COVID-19: Perspectives from North Africa*
21 | 02 Jean-Pierre Darnis, *Le relazioni transatlantiche al tempo del digitale: la questione del trasferimento di dati*
21 | 01 Arnout Molenaar, *Unlocking European Defence. In Search of the Long Overdue Paradigm Shift*
20 | 48 Massimiliano Frenza Maxia, *Blockchain statale e yuan digitale: "game changer" di Pechino nella competizione imperiale con gli Usa?*
20 | 47 Alessandro Picchiarelli, *Per un'intelligenza artificiale a misura d'uomo: una possibile regolamentazione valoriale?*
20 | 46 Diego Todaro, *Tecnologia e azione pubblica in Cina: il codice sanitario individuale e le principali tendenze delle politiche digitali cinesi contemporanee*
20 | 45 Rose Gottemoeller and Steven Hill, *NATO's Current and Future Support for Arms Control, Disarmament and Non-proliferation*
20 | 44 Wilfred Wan, *Nuclear Risk Reduction: Looking Back, Moving Forward, and the Role of NATO*

ISSN 2610-9603 | ISBN 978-88-9368-176-6 © 2021 IAI