Istituto Affari Internazionali

Italy and Cyber Defence

by Alessandro Marrone, Ester Sabatino and Ottavia Credi

ABSTRACT

Cyber defence has gained a growing relevance in Italy, as a result of a high number of serious attacks against private entities, the armed forces and the public administration – as in the case of the Lazio Region in 2021. Italy has addressed the problem with the creation of the Network Operations Command (*Comando per le Operazioni in Rete* – COR) within the national defence framework, and with a broader reform of the sector's governance that led to the definition of the National Cybersecurity Perimeter and the institution of the National Cybersecurity Agency (*Agenzia per la Cybersicurezza Nazionale* – ACN). At the international level, major NATO Allies as well as the Alliance as a whole are developing their own approach to cyber defence, in the context of a strategic and doctrinal debate over a new operational domain characterised by exceptional features. The disruptive roles acquired by technology and the private sector in this domain demand new forms of dialogue and collaboration between the institutions and the national industry.

Cyber security | *Defence policy* | *Italy* | *NATO*

keywords

DOCUMENTI IAI 21 | 12EN - SEPTEMBER 2021

ISSN 2280-6164

Italy and Cyber Defence

by Alessandro Marrone, Ester Sabatino and Ottavia Credi*

[*] Alessandro Marrone is the Head of the Defence Programme at Istituto Affari Internazionali (IAI). Ester Sabatino has been a Researcher in IAI's Defence Programme until 31 August 2021. Ottavia Credi is a Junior Researcher in IAI's Defence and Security Programmes. The authors would like to thank Danilo Mattera, Intern in IAI's Defence Programme from September until December 2021, for his support.

· This study was written as preparation for the close-door seminar "La cyber defence in Italia: sviluppi in rete" organised by IAI on 21 July 2021 with the support of Elettronica, and was then reviewed taking to account the debate that was held during the event.

ISSN 2280-6164

Introduction

In recent years, cyber defence gained a growing relevance at national and international level, as a result of an increased number of cyberattacks. According to some estimates,[1] in the first semester of 2020 alone, over one-sixth of the 850 serious cyberattacks registered globally affected public entities. In the same period, attacks against critical infrastructures increased by 85 per cent, if compared to the same period in the previous year. This trend was observed also in Italy, with over 500 reports of attacks against infrastructures of national relevance reported in 2020, while approximately 147 were reported in 2019.[2] The increase in the number of attempts to steal data, interrupt services, and jeopardise technological infrastructures is even more alarming given the variety of actors involved in the perpetration of these attacks, delivered by state as well as non-state actors.

Recent cyberattacks with international consequences shed light on the potentialities and risks to security in cyberspace. That was, for instance, the case of the ransomware attack against the software produced by the American firm Kaseya in July 2021, and the attack against the Lazio Region in Italy. In cyberspace, there is no internationally agreed legislation, nor limitation to the proliferation of systems that might be employed, also due to the inherent dual use nature of such devices.

From a defence perspective, the cyber domain represents a challenge to be faced and an opportunity to be seized and thus deserves serious attention. In the military context, defence against potential cyberattacks may involve different structures, including the personnel deployed in international operations, systems and equipment, armed forces both on national territory and abroad, and the protection of information with strategic relevance and the actual defence against cyberattacks – be they targeting military structures or the security of a state as a whole. In the framework of the Atlantic Alliance, a cyberattack might trigger the activation of the principle of collective defence, established by Article 5, with possible consequences also in the "real world". Against this backdrop, NATO is working on the creation of a shared approach among its member states. However, Allies differ in terms of national structures and capabilities for cyber defence, and national posture regarding possible response operations.

This is the context in which Italy's cyber defence operates. The Network Operations Command (*Comando per le Operazioni in Rete* – COR), established in 2020 and characterised by a joint nature, is tasked with countering cyberattacks against national Defence structures and potential attacks of national relevance. However, similarly to other states that are of interest to Italy, Italian cyber defence is only

[1] See, among others: Associazione Italiana per la Sicurezza Informatica, *Rapporto CLUSIT 2020 sulla sicurezza ICT in Italia*, October 2020, p. 20, https://clusit.it/wp-content/uploads/download/Rapporto-Clusit_2020_web_ottobre.pdf.

[2] Italian Senate, *"Agenzia per la sicurezza nazionale. Asset strategico per l'Italia digitale" Convention*, Rome, 6 July 2021 (video), https://youtu.be/jxJXK9XmlPo.

ISSN 2280-6164

one element of the much wider cyberspace security context. In such framework, a variety of actors – first and foremost the new National Cybersecurity Agency (*Agenzia per la Cybersicurezza Nazionale* – ACN) – is required to intervene in various ways, in order to enhance state resilience, its capability to respond to cyber crises and its rapidity of action. This study aims to provide an in-depth, broad-spectrum analysis of cyber defence in Italy, framing it in the NATO context and highlighting the main developments of the new national institutional framework, with special attention to the approach of the Ministry of Defence (MoD), the strategic aspects of this domain, and the steps that the national economic system could take towards a coordinated and comprehensive response to cyber threats.

1. The Italian institutional and legislative framework

by Ester Sabatino

The Italian institutional and legislative framework governing cybersecurity is currently in the making, and it is being developed around the ACN, established with the Decree-Law No. 82 of 14 June 2021,[3] passed with amendments into law No. 109 of 4 August 2021.[4] Such legislative developments demonstrate Italy's growing acknowledgement of the complexity of the cyber threat, starting with the tight connection between the state's cybersecurity and national defence.[5] In order to gain a better understanding of the state of the art, this chapter provides a brief description of the main normative developments which have outlined the legislative and institutional framework for cybersecurity in Italy since 2013, as well as an analysis of the newly-established Agency.

1.1 Evolution of the normative framework in Italy from 2013 to 2020

In Italy, cyber defence is set within the broader cybersecurity framework. Following a series of initiatives at the European Union and NATO level, Italy established its first structure for national cybersecurity and critical infrastructures protection through a Decree of the President of the Council of Ministers (*Decreto del Presidente del Consiglio dei Ministri* – DPCM) of 24 January 2013, also known as *Decreto Monti*.[6]

The *Decreto Monti* identified the Security Intelligence Department (*Dipartimento delle Informazioni per la Sicurezza* – DIS) as the entity tasked with the protection of Italy's cybersecurity, notwithstanding that the tasks identified by Decree are actually different from the duties historically carried out by the DIS as an intelligence agency. The Decree also established the National Cybersecurity Management Board (*Nucleo per la Sicurezza Cibernetica* – NSC), aimed at providing operative support in the event of cyber crises of national relevance, and an inter-ministerial board responsible for the prevention and management of such crises. Moreover, according to the Decree, the Interministerial Committee for the Security of the Republic (*Comitato Interministeriale per la Sicurezza della Repubblica* – CISR) was in charge of advising the President of the Council of Ministers concerning the

[3] Italy, Decree-Law No. 82 of 14 June 2021: *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg.

[4] Italy, Law No. 109 of 4 August 2021: *Conversione in legge, con modificazioni, del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*, https://www.gazzettaufficiale.it/eli/id/2021/08/04/21G00122/sg.

[5] Italian Senate, *Risoluzione approvata dalla Commissione sull'affare assegnato n. 423*, 7 April 2021, http://www.senato.it/japp/bgt/showdoc/18/SommComm/0/1210625/index.html?part=doc_dc-allegato_a:1.

[6] Presidency of the Council of Ministers, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, 24 January 2013, https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg.

national strategic framework for cyberspace and cybersecurity strategic objectives, through the National Plan for Cyberspace Protection and ICT Security (*Piano nazionale per la sicurezza dello spazio cibernetico*). In addition, the CISR had to elaborate guidelines for possible cooperation between public and private entities, disseminate best practices for cyberspace protection, and advocate activities aimed to ensure an Italian presence in international cooperative frameworks, including NATO and the EU. The CISR was assisted by the Technical Committee for the Security of the Republic (*Comitato Tecnico Interministeriale per la Sicurezza della Repubblica* – CISR tecnico), a joint coordination board.

The Italian cybersecurity institutional and normative framework evolved according to the DPCM of 17 February 2017 (*Decreto Gentiloni*),[7] then followed by the National Plan for Cyberspace Protection and ICT Security (*Piano nazionale per la protezione cibernetica e la sicurezza informativa*).[8] The need to rationalise and simplify a complex institutional landscape, in an attempt to create synergies and economies of scale in a coordinated fight against the cyber threat, led to the evolution of the national cyber architecture.

Following the implementation of the *Decreto Gentiloni*, the DIS gained further duties and became both an operative actor of the cybersecurity structure and an entity responsible for defining guidelines in order to safeguard this domain and respond in the event of crises. The relocation of the NSC represented one of the changes that led to the strengthening of the DIS: formerly integrated within the Prime Minister's Military Advisor Office (*Ufficio del Consigliere militare della Presidenza del Consiglio*), the NSC is incorporated within the DIS, chaired by its Deputy Director. Among its tasks, the NSC has to facilitate the liaison between the different actors involved in the national cybersecurity architecture, as well as managing crises in cyberspace.

A further and relevant change introduced by the decree consists in the establishment of a National Centre for Evaluation and Certification (*Centro di valutazione e certificazione nazionale* – CVCN).[9] The CVCN is tasked with verifying security standards of technological products that will be employed within national critical infrastructures.[10] The relevance of private entities for the determination of national cybersecurity levels was already acknowledged in the *Decreto Monti*.

[7] Presidency of the Council of Ministers, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, 17 February 2017, https://www.gazzettaufficiale.it/eli/id/2017/04/13/17A02655/sg.

[8] Presidency of the Council of Ministers, *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, March 2017, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf.

[9] The Centre was established in 2019. For further information, see: Ministry of Economic Development, *Istituito il Centro di valutazione e certificazione nazionale (Cvcn)*, 19 February 2019, https://www.mise.gov.it/index.php/it/198-notizie-stampa/2039261.

[10] Stefano Mele, "Le tre novità che cambieranno la cyber security nazionale, con il nuovo decreto", in *Agenda Digitale*, April 2017, https://www.agendadigitale.eu/?p=30583.

Such awareness led to the drafting of the Decree-Law No. 105 of 21 September 2019, defining the National Cybersecurity Perimeter[11] according to the procedures later defined by the DPCM No. 131 of 30 July 2020.[12] Among the different duties[13] of the operators,[14] there is the need to certify the products and services they use. The certification ought to be implemented by the CVCN, according to the procedures defined above.[15] All these actions contribute to the strengthening of the national security architecture and the greater resilience of operators and providers of essential public services. This is allowed by the employment of information and communications technology (ICT) assets, products and services that should be designed in a way that ensures they are secure and resistant against cyber threats, namely secure by design. Against this backdrop, it is important to emphasise how the MoD has not yet been assigned a specific role in the country's legislative framework, despite the label of "cornerstone" of the National Cybersecurity Perimeter it gained over time, especially with the Decree-Law 105/2019. This might prevent the armed forces from receiving the appreciation they deserve for the capabilities they provide in the protection of the national cyberspace, also considering the ongoing developments at NATO level and among major western Allies, which also involved the MoD through the recent establishment of the COR.

1.2 The current institutional and legislative framework and the National Cybersecurity Agency (ACN)

The national legislative framework on cybersecurity has been further regulated by the Decree-Law 82/2021. Amended by law, the decree introduces several changes to the national cybersecurity architecture, such as the establishment of the ACN.[16] The institution of the Agency is one if the initiatives implemented through the Italian Recovery and Resilience Plan (*Piano nazionale di ripresa e resilienza* – PNRR),[17] which the MoD intends to support through its expertise and the structures

[11] Italy, Decree-Law No. 105 of 21 September 2019: *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*, https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg.

[12] Presidency of the Council of Ministers, Decree No. 131 of 30 July 2020: *Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*, https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg.

[13] For further information, see: Presidency of the Council of Ministers, Decree No. 81 of 14 April 2021: *Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza*, https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg.

[14] The Perimeter has been increased by the Prime Minister Mario Draghi on 15 June 2021. For further information, see: Presidency of the Council of Ministers, *Cyber: aggiornato l'elenco dei soggetti del "perimetro di sicurezza cibernetica nazionale"*, 15 June 2021, https://www.governo.it/it/node/17154.

[15] Italian Presidency, Decree No. 54 of 5 February 2021: *Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*, https://www.gazzettaufficiale.it/eli/id/2021/04/23/21G00060/sg.

[16] Italy, Decree-Law No. 82 of 14 June 2021, cit. Roberto Baldoni is appointed as Agency Director while Nunzia Ciardi is appointed as Agency Deputy Director.

[17] Cybersecurity is one of seven investiments aimed at digitalising the public administration.

at its disposal.[18]

The law establishes regulatory, administrative, patrimonial, organisational, accounting and financial independence of the Agency, while the President of the Council of Ministers holds the high management and the general responsibility of national cybersecurity policies (Article 2). The ACN is tasked with the preparation of an annual report, submitted to Parliament by the President of the Council of Ministers. To allow the Agency to start functioning, the decree sets up a budget of 2 million euro for the year 2021 and an aggregate budget of 529 million euro for the 2021-2027 period (Article 18). These financial assets should also cover the salaries of the 300 officials that will ensure the Agency's initial functioning, and whose salaries will be standardised to those of the officials of the Bank of Italy. By doing so, the Government aims to raise the attractiveness of the public sector, which is often unable to offer wages and career opportunities as enticing as those granted by the private sector in the field of cybersecurity. This problem affects Italy as it does other European countries, with relevant implications also for the Italian armed forces.

Among the major changes introduced by the Decree-Law is the relocation of the national cybersecurity architecture from the DIS to the ACN, still governed by public law, which will report directly to the President of the Council of Ministers. The ACN will work closely with the Intelligence System for the Security of the Republic (*Sistema di informazione per la sicurezza della Repubblica*) through the Cyber Security Unit (*Nucleo per la cybersicurezza*), namely the institution established to replace the NSC. The Unit encompasses the ACN Director General and Deputy Director, the Prime Minister's Military Advisor, representatives of the DIS, of the Internal Intelligence and Security Agency (*Agenzia Informazioni e Sicurezza Interna* – AISI) and of the External Intelligence and Security Agency (*Agenzia Informazioni e Sicurezza Esterna* – AISE), all Ministers involved in the CISR,[19] and representatives of the Ministry of University and Research, of the Ministry for Technological Innovation and Digital Transition and of the Civil Protection Department. The Unit is responsible for organising and planning the response in the event of cyber crises, as well as coordinating interministerial exercises and the Italian participation in international drills.[20] It should be stressed that the Unit receives reports of security violations and attempts thereof against state information technology (IT) systems as well as notifications from the

Around 620 million euro will be devoted to the creation of a cybersecurity infrastructure but also to strengthen operative structures and increase national cyberdefence capabilities. For further information, see: Presidency of the Council of Ministers, *Piano nazionale di ripresa e resilienza*, May 2021, https://www.governo.it/sites/governo.it/files/PNRR.pdf.

[18] Senate of the Republic, *Risoluzione approvata dalla Commissione sull'affare assegnato n. 423*, cit.

[19] The CISR is composed by: the President of the Council of Minister, the Delegated Authority (Autorità Delegata),the Minister of Foreign Affairs, the Minister of the Interior, the Minister of Defence, the Minister of Justice, the Minister of Economy and Finance, the Minister for Economic Development and the Minister for Ecological Transition.

[20] It should be noted that Article 9(1)(c) does not specify whether international exercises also include defence exercises.

Computer Security Incident Response Team (CSIRT) Italia,[21] thus allowing the gathering of a considerable amount of data. Moreover, the Unit assesses the nature and the intensity of the cyber events affecting national infrastructures or national relevance that require a coordinated response.

The Agency is the sole national reference institution in cybersecurity, and it is responsible for the drafting of the national cybersecurity strategy and for ensuring the regular development of common actions meant to reach higher levels of national resilience. The ACN takes on all functions related to the national cybersecurity Perimeter, and operates as the cybersecurity certification authority, superseding the CVCN with respect to products and services acquired by subjects within the Perimeter. In addition, the Agency acts as the national point of contact as required by Directive (EU) 2016/1148, as well as the National Coordination Centre as required by the Regulation (EU) 2021/887.[22]

The conversion into law of the Decree-Law implies important ramifications on the national cybersecurity architecture in general, and the Perimeter in particular, with respect to cloud services and cryptography. Regarding the former, the ACN will have to provide the certification of cloud services used by the public administration, which are currently considered unsafe.[23] As far as cryptography is concerned, the Agency will undertake essential activities in order to promote it as a cybersecurity tool, carrying out actions considered necessary to strengthen Italian industrial and technological autonomy.

Some of the duties previously covered by the CISR are now fulfilled by the Interministerial Committee on cybersecurity (*Comitato Interministeriale per la Cybersicurezza* – CIC), now tasked with advising, proposing and supervising cybersecurity, as well as adopting the national cybersecurity Perimeter's implementing acts and suggesting subjects that may be included in it. Yet, the CISR retains responsibilities concerning potential serious and impending risks for network security. In this case, according to Article 5 of Decree-Law 105/2019 and after a CISR deliberation, the President of the Council of Ministers may decide to disable devices and products used in the network that are deemed to be at serious risk.

The content of the Decree-Law suggests particular attention towards private entities and education, made clearer through dedicated amendments added as it was converted into law. With respect to private entities, the Agency will be able to stipulate bilateral and multilateral agreements involving the private sector

[21] The CSIRT Italia is the new denomination of Italian CSIRT established according to the implementing decree of Directive (EU) 2016/1148.

[22] European Parliament and Council of European Union, *Regulation (EU) 2021/887 of 20 May 2020, that established the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*, https://eur-lex.europa.eu/eli/reg/2021/887/oj.

[23] Gabriele Carrer, "Sì della Camera all'Agenzia cyber. Le novità del disegno di legge", in *Formiche.net*, 28 July 2021, https://formiche.net/?p=1407072.

in order to foster the development of industrial and technological capabilities and expertise, possibly also through the involvement of academia and research institutions. Through the Decree-Law's conversion into law, an amendment introduced the establishment of a Technical-Scientific Committee aimed to assist the Agency through proposals and consultations, also in the fulfilment of tasks and the management of activities of the private sector. The Committee will be made of representatives of the industrial sector, think tanks, academia, research institutions and trade associations. Hopefully, their involvement suggests further dialogues among the involved parties in the future, favouring the coordination of their respective activities with the ultimate aim of ensuring a higher degree of cybersecurity.

When it comes to education, the Agency will proceed on two trajectories. The first, and more general, will raise awareness about cyber threats through communication campaigns aimed at increasing the cybersecurity knowledge at national level. The second trajectory will concern advanced training of qualified personnel through specific academic courses; moreover, it will work towards the creation of structures dedicated to innovation development via staff training and recruitment. As in the case of major European countries and Allies,[24] the civil population's inability to identify cyber threats, coupled with experts' insufficient technical and professional skills, might be an obstacle for the prevention of and response to cyberattacks.

The current set up prescribes that, in the event of an attack, the Cyber Security Unit would be the entity called to intervene. Representatives from relevant ministries will coordinate in order to ensure a common response. Given the uncertainty of borders in cyberspace, in the event of a crisis the Unit contacts its international counterparts to ensure the correct management of the situation, including NATO and other international organisations of which Italy is a member.[25]

With specific reference to this aspect, it is important to emphasise that the Decree-Law did not attribute a specific role to the MoD in the context of the duties ascribed to the ACN. While the text of the Decree-Law did envisage a relation with the Ministry of Foreign Affairs and International Cooperation regarding international cooperation on cybersecurity (Article 7, para. 3(q)), the peculiarities of the MoD were not equally acknowledged in the context of the armed forces and the Italian participation to cooperation frameworks and security organisations. The MoD only detained the authority, as entitled entity, to grant the European cybersecurity certificate, namely the certification attesting the legitimacy of ICT products as established by the Regulation (EU) 2019/881 (Article 7). The sector's specific features were then taken more into account by amendments introduced during the Decree-Law's conversion into law. The conversion law clarifies the need for a relation with the MoD on different subject matters, first and foremost the Italian participation to projects and initiatives in collaboration with NATO and the European Defence

[24] For further information, see chapter 5 of this study.

[25] Italy, Decree-Law No. 82 of 14 June 2021, cit., Article 10.

Agency (EDA), which would draw further attention to aspects related to military research and sectoral training thanks to highly specialised expertise provided by the armed forces.

2. The Network Operations Command (COR)

by Alessandro Marrone and Ottavia Credi

In general, the MoD has its own and well-defined role and duty to preserve the national interest abroad, as demonstrated by Italy's participation in international missions. Moreover, the MoD has the enduring requirement to protect its info- and infrastructural assets, starting from its online network.

In this context, and according to the normative and legislative framework outlined in the first chapter, the Network Operations Command (*Comando per le Operazioni in Rete* – COR) is undoubtedly among the major relevant actors in the national cyber defence scheme. The COR is a joint command established in February 2020 under Italian Defence General Staff, tasked with the coordination of cybersecurity and cyber defence activities of the armed forces and the MoD.[26]

2.1 Origins and premises

Among the reasons that led to the establishment of the COR, two are particularly important. On the one hand, the creation of this structure was driven from the necessity to have a sole command that would encompass the capabilities needed to operate in cyberspace. This includes ICTs, command, control, communication and computers (C4), intelligence, and surveillance and recognition (ISR) capabilities. This is particularly relevant as a way to incorporate competences and responsibilities which used to be fragmented into one single command characterised by a unified vision and a more operative setting. Even more so for units working on the ICTs and C4 components of the MoD, as well as those responsible for conducting operations in the cyber domain – as will be further explained in the next paragraph.

On the other hand, the COR resulted from the willingness to reach a higher level of efficiency and rationalisation of the MoD's technical and operative structure, also to promote an even more cooperative and consolidated relationship among the armed forces. In this sense, the COR is part of a long-lasting and difficult process aimed at encouraging the adoption of a joint approach on behalf of all armed forces, in order to take advantage of their expertise within a more effective and efficient chain of command. Such a joint approach is even more important considering the growing interest demonstrated by both Allies and strategic competitors in multi-domain operations, in which cyberspace is considered an operational domain equal to others, thus requiring a sole command that has to be responsible for cyber operations.

The Chief of Defence Staff's 2020 Strategic Concept (*Concetto Strategico del Capo di Stato Maggiore della Difesa* – CASMD), concentrates on the need to improve

[26] For further information, see Italian MoD website: *Comando per le Operazioni in Rete (COR)*, https://www.difesa.it/SMD_/COR. The COR is lead by Vice Admiral Ruggiero Di Biase.

joint and multi-domain operations, and provides a set of guidelines about the approach that the armed forces should adopt to conduct operations in cyberspace.[27] In particular, the CASMD identifies seven essential pillars characterising this domain: the identification of vulnerabilities; the strengthening of resilience; the integration of the actors operating in the cyberspace, both within the national territory and abroad; deterrence, intended both as capability and as intention to conduct operations in the cyberspace; the ability to react in a timely manner to cyberattacks; technological development, facilitated by investments in research and development and possibly the engagement of start-up or small and medium sized enterprises; and the achievement of a cyber awareness aimed at establishing an informed approach to the cyber domain as well as obtaining information and specific competences for the development of new capabilities.

Starting from these premises, a timely, long-term planning supported by appropriate investments led to the establishment of the COR.

2.2 Organisational chart and specific duties

The COR is supervised by the CASMD, and works in collaboration with the cyber defence and cybersecurity units of the Army, the Navy and the Air Force.

The Command is organised in three Divisions: the C4 Division, the Security and Cyber defence Division, and the Cyber Operations Division.[28]

The C4 Division inherited the competences previously offered by the Joint C4 Command (*Comando interforze C4 Difesa* – C4D), thus taking over the governance of the Defence Network (*Rete della difesa* – DIFENET) and the management of the ICT capabilities of all armed forces' general staffs. This was allowed by the integration of the competences of the Security Operation Center (SOC), the Network Operation Center (NOC) and the Infrastructure Operation Center (IOC) in a sole structure, namely the ICT Operativity Office (*Ufficio Operatività ICT*). Within C4 Division operates the Network and Data Centre Office (*Ufficio Reti e Data Center*), which works to assure the continuity of Defence activities – in industry terms, "business continuity" – and recovery in the event of serious crises – in other terms, disaster recovery. Currently, the Division counts on 12,000 km of the National Optical Fiber Joint Network (*Rete Interforze in Fibra Ottica Nazionale* – RIFON) and 10,000 km of radio links composing the Numerical Joint Network (*Rete Numerica Interforze* – RNI) and the Metropolitan Area Network (MAN) of Rome. Besides ensuring efficiency, monitoring and constant support of C4 services, the Division is also involved in planning, development and implementation activities, led by the Centralised Systems and Applications Office (*Ufficio Sistemi e Applicativi Centralizzati*).

[27] Italian Defence General Staff, *Il Concetto Strategico del Capo di Stato Maggiore della Difesa*, January 2020, https://www.difesa.it/SMD_/CaSMD/concetto_strategico_casmd.

[28] See Italian MoD website: *Reparto C4*, https://www.difesa.it/SMD_/COR/Pagine/reparti.aspx.

The Security and Cyber defence Division is tasked with the development of a national cyber defence architecture and systems aimed at safeguarding ICT infrastructures. To this end, the Division's activity is threefold: the identification of capabilities to strengthen the aforementioned national cyber defence architecture; the systematic monitoring of relevant activities taking place in cyberspace, whilst assessing its vulnerability; and the development of strategies to prevent potential threats in cyberspace. The Computer Emergency Response Team (CERT) continues to operate within the Division; it is a structure operating 24/7 that has considerably improved its capabilities over the years. Currently, the CERT also conducts preventive activities such as the development of threat intelligence capabilities for the armed forces, namely the collection and analysis of information related to cyber threats that affect or might affect these structures.

The Division also encompasses the Security Infrastructures Office (*Ufficio Infrastrutture di Sicurezza*), aimed at the development of security systems conceived, designed and realised according to the security and cyber defence needs, following the principle of security-by-design. This element is particularly significant because the vast majority of current ICT devices, just like the Internet, were not developed according to such principle. Rather, security needs tend to only be considered *ex post*, through the strengthening of specific elements' defence capabilities. The Security Infrastructures Office is also responsible for assessing cyber risks and handling different validation processes. Such competence is potentially very relevant, also given the security certification function assigned by the current normative framework to the MoD, as well as the activities once carried out by the CVCN and currently covered by the ACN. Finally, within the Division, the Classified Systems Office (*Ufficio Sistemi Classificati*) works to strengthen and reinforce C4 classified services.

The Cyber Operations Division derives from the integration of the former Joint Command for Cyber Operations (*Comando Interforze per le Operazioni Cibernetiche* – CIOC) within the COR.[29] It manages all military activities carried out in cyberspace for the protection of the MoD's systems and services from cyber threats, both within the national territory and in theatres of operation abroad. In this context operate the Cyber Operation Cells (*Cellule Operative Cibernetiche* – COCs), formerly established within the CIOC and now part of the COR's Cyber Operations Division.[30] COCs are teams made of experts from all the armed forces, able to conduct offensive and defensive operations in order to decrease the vulnerability of both cyber infrastructures both in Italy and deployed personnel participating in international operations. For instance, the COC deployed in Peja,

[29] The CIOC, established by National Plan for Cyberspace Protection and ICT Security in 2017, was tasked with the protection of MoD systems and networks from cyber threats.

[30] Italian Chamber of Deputies-Defence Commission, "Indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico", in *Resoconti stenografici*, 20 December 2017, p. 32, http://documenti.camera.it/leg17/resoconti/commissioni/bollettini/pdf/2017/12/20/leg.17.bol0935.data20171220.com04.pdf.

Kosovo, is tasked with the defence of non-classified networks used by the national troops to conduct defensive cyber operations.[31] Also because of their presence on the battlefield, COCs could be employed in crisis scenarios, providing a more specific and rapid response.[32]

As in the case of the former CIOC,[33] the new Division manages the education and recruitment of personnel, the analysis of threats, the protection of IT infrastructures, and the innovation of the MoD's approach to cyber defence and technological procurement. Once again, the Division is organised in three different offices. Among their tasks, the Operations Office (*Ufficio Operazioni*) and the Cyber Activities Offices (*Ufficio Attività Cibernetiche*) conduct the so-called penetrations tests, namely simulations of cyber intrusions designed to assess the resilience level of the MoD's IT systems. The two offices also collaborate with partner countries as well as with experts from Italian academia. Finally, the Army Training & Lessons Learned Office (*Ufficio Addestramento Esercito & Lessons Learned*) trains external personnel to operate in cyberspace.[34]

Given the growing relevance of the human factor in such an innovative domain, the education of human resources represents a pivotal element.[35] Against this backdrop, the Defence General Staff recently proposed the establishment of a Cyber Defence Academy: a federated educational system which could gather education centres from different ministries in order to integrate, organise and harmonise education activities on the cyber domain.[36] Furthermore, the MoD is currently assessing a Concept Paper drafted by the COR examining the Command's own recruiting procedures.[37] Besides recruitment and education, it is important to address the issue of information: due to the predominance of the cyber domain in modern society, it would be timely to spread general knowledge about the cyber domain beyond cyber experts, in order to strengthen Italy's overall level of cyber

[31] The aforementioned COC has been deployed in Kosovo as part of KFOR Operation, within the broader NATO Joint Enterprise mission. For further information, see Italian MoD: *Kosovo - KFOR - Joint Enterprise*, https://www.difesa.it/OperazioniMilitari/op_intern_corso/KFOR.

[32] Interview, 21 July 2021.

[33] On former-CIOC activies, see the Chief of Defence Staff's interview: "Cyber Defence. Nasce il Comando Interforze per le Operazioni Cibernetiche", in *Informazioni della Difesa*, No. 3/2017 (March 2017), p. 8-10, https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/ID-3_2017_ridotto.pdf.

[34] The Cyber Range, established in 2016 and still in development, has been created with the aim of increasing the expertise of these resources. The Cyber Range is a Defence virtual framework which implements cyberattack simulations in order to assess national defence capabilities in cyberspace. For further information on the Cyber Range, see Alessandro Armando, "Cyber Range. Attacco e difesa in ambiente simulato", in *Gnosis*, No. 2 (February 2016), p. 67-73, http://gnosis.aisi.gov.it/gnosis/Rivista47.nsf/ServNavig/47-26.pdf/$File/47-26.pdf.

[35] Lieutenant General Enzo Vecciarelli during the conference *"Agenzia per la sicurezza nazionale. Asset strategico per l'Italia digitale"*, cit.

[36] Italian MoD, *Il Sottosegretario Mulè al webinar dedicato alla Cybersecurity*, 17 May 2021, https://www.difesa.it/Primo_Piano/Pagine/Il-Sottosegretario-Mule-al-webinar-dedicato-alla-Cybersecurity.aspx.

[37] Interview, 21 July 2021.

resilience and cyber defence.

2.3 Advantages, potentialities and open issues

The establishment of the COR led to several advantages in terms of the armed forces' capabilities to assure growing levels of cyber defence. First of all, the COR grants the Defence General Staff, the Italian Joint Operations Headquarters (*Comando Operativo di Vertice Interforze* – COI) and the Joint Special Forces Operations Headquarters (*Comando interforze per le Operazioni delle Forze Speciali* – COFS) easier access to information in or about cyberspace. In particular, the COR is the primary cyber component of the COI, in accordance with the trend of encompassing operations in all operational domains under a higher joint Command.[38]

Secondly, the activity the COR is conducting to develop technological capabilities and human resources for the MoD suggests the possible enhancement and reinforcement of the Italian military competences in cyberspace. For instance, through forensic IT skills, the COR will facilitate the attribution of cyberattacks, with positive implications for the prevention and repression of cybercrimes and for the implementation of an effective deterrence in the cyber domain.[39] As demonstrated by the duties assigned to the COCs,[40] the COR aims to bring about developments for the MoD – through the so-called "preventive cyber operations" – as well as strengthen its capabilities to conduct offensive operations.[41]

Both the operative and the capacitive development dimension benefit from the exercises organised by the COR. Through the testing of expertise on the one hand, and procedures on the other, these exercises contribute to improving both aspects via first-hand experience.

Considering the limited role played by the MoD within the current normative framework regulating national cybersecurity,[42] the establishment of the COR represents an opportunity for the Ministry to enhance its collaboration with the national cybersecurity architecture, operating as a joint contact point for the ACN and the other actors involved. Yet, whether or not this opportunity will be seized will heavily depend on the approach that the ACN will adopt, the dynamics that will form within the Unit and, in general, the transformation that will occur within

[38] Italian MoD website: *Il Comando Operativo di Vertice Interforze (COVI)*, https://www.difesa.it/SMD_/COI.

[39] Lieutenant General Enzo Vecciarelli during the conference *"Agenzia per la sicurezza nazionale. Asset strategico per l'Italia digitale"*, cit. Forensic information technology uses digital data to prove informatic evidences for investigative purposes. For further information on attribution, see chapter 3.

[40] Italian Chamber of Deputies-Defence Commission, "Indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico", cit.

[41] For a brief overview on operations that could be conducted in Italia, see chapter 5.

[42] See chapter 1.

the national cybersecurity Perimeter.

The activities conducted by the Command provide the MoD with more opportunities to interact with representatives from the industrial sector and academia – an essential element to ensure a constant improvement and update of the COR's own capabilities, and therefore the MoD's. Given the nature of cyberspace, this process can only occur through regular exchanges with the most innovative and cutting-edge civilian entities. To this end, it is necessary to encourage an all-encompassing and unvarying strengthening of cyber defence and cybersecurity.[43] Also in this case, the complete fulfilment of the COR's potential will depend partly on the role that the ACN will play, and partly on the synergies that will be fostered between the Agency and the Command.

Finally, considering Italy's relation with NATO, the COR currently represents the leading actor for the definition of cyber defence standards. Through the establishment of the COR, the Ministry has been able to align itself to NATO guidelines and interact with the Cyber Operation Command (CYOC) and other NATO entities.[44] The mandate of the ACN remains an open issue since, by indicating the Agency as the sole international point of reference, seems to include relations with NATO as well as with the EU.

Another open issue concerns the personnel employed and employable in the COR now and in the mid-term, from two different perspectives. Delays in reaching full operational capability (FOC) suggest difficulties in finding human resources among the current military staff which may be suitable for operating in cyberspace. For the Command to ensure a high level of preparedness of its personnel, it will need to continue investing in educational activities on cyber defence and cybersecurity, for both employees and managers, possibly in synergy with other existing organisations.[45] The quality of personnel is a crucial factor since, through the COR, the MoD can gain further freedom of action in the cyber domain, possibly enhancing its ability to conduct different types of cyber operations in an autonomous manner.

Through time, the COR will need to ensure an appropriate flow of human resources; also, it will need to work on preserving them long enough to guarantee the continuity and growth of common competences, and on facilitating a staff turn-over that will take advantage of younger recruits' natural inclination towards technology and cyberspace. Given the attractiveness of the private ICT sector

[43] Interview, 4 June 2021.

[44] NATO architecture will be debated in chapter 3.

[45] In this sense, there are already two different structures dedicated to the education of military staff on cyber defence. The first is the Armed Forces Institute of Telecommunications (*Scuola Telecomunicazioni Forze Armate* – STELMILIT) established in Chiavari; the second is the *Laboratorio Addestrativo per la Difesa Cibernetica* (LADC) sets within Italian Army's Scuola delle trasmissioni. The establishment of this structure symbolised the first step toward the creation of Italian Army's Cyber Security Department (*Reparto di Sicurezza Cibernetica* – RSC).

in terms of salary and benefits, and the partial lack of Italian graduate experts in science, technology, engineering and mathematics,[46] the armed forces in general and the COR in particular will need to implement appropriate economic incentives and opportunities for professional growth.[47] In other words, the COR will need to demonstrate its ability to face – or at least mitigate – systemic problems affecting the recruitment process and the maintenance of the personnel working in the national cyber defence system.

2.4 The joint integration issue

Over the past few years, integration efforts within the cyber domain experienced relevant improvements at joint level, as demonstrated by RIFON's technological developments.[48] A joint centralisation indeed benefits all armed forces: once there is a shared agreement about information sharing, as well as the respective responsibilities, an environment of appropriate operative conditions and common trust allows the creation of a shared picture – much more useful than the partial pictures provided by each armed force.

Against this backdrop, there are still a few open issues – first and foremost, an insufficient level of data sharing and cooperation among structures. The standardisation process is still partially incomplete; yet, this is a particularly important operation since reaching an agreement over a set of standards can lead to a higher degree of operative integration, with positive comebacks also at strategic level.[49] Threat intelligence activities have not yet reached an optimal joint level.[50] Furthermore, despite the merging of structures and expertise within the COR, the armed forces' CERTs continue to operate. This raises the issue of finding a way to assure the best possible cooperation, efficacy and efficiency within the national cyber defence architecture. The CERTs operating within the Army, the Navy and the Air Force resort to the same systems for anomaly detection within the network, namely Security Information and Event Management (SIEM) devices, which raise the alarm in the event of a cyberattack. This allows tangible data sharing, through which it is possible to achieve a common picture.[51] Still, there is a lot of room for improvement, and it is crucial to avoid investment fragmentation and duplication within the armed forces.[52] Lastly, the latest Plurennial Programmatic Document (*Documento programmatico pluriennale* – DPP), presented by the MoD,[53] urged the creation of a coherent cyber defence system, which should ensure interoperability

[46] Interview, 5 July 2021.

[47] Interview, 26 May 2021.

[48] Interview, 21 May 2021.

[49] Interviews, 21 May and 27 May 2021.

[50] Interview, 27 May 2021.

[51] Interview, 21 May 2021.

[52] Ibid.

[53] Italian MoD, *Documento Programmatico Pluriennale della Difesa per il Triennio 2020-2022*, 2020, p. 44, https://www.difesa.it/Content/Documents/DPP/DPP%202020-2022.pdf.

with the model developed by the Atlantic Alliance.

Working towards this objective, joint integration will represent an essential factor, since it guarantees a united Italian front able to relate with representatives of allied countries and NATO entities. Achieving joint integration will not, however, be sufficient – what is also needed is further understanding of ongoing developments within the framework of the Alliance.

3. Developments in the NATO framework

by Ottavia Credi

With the aim of advancing its cyber defence capabilities, NATO is developing a shared and synergetic approach within its members, commands and agencies. With the official recognition of cyberspace as an operational domain, NATO intends to integrate cyber operations in support of allied military operations, enhance the security standards of its members, initiate cooperative initiatives with partner countries, and contribute to the development of the international law governing the cyber domain.

3.1 The evolution of the allied approach

NATO's focus on cyber defence intensified in response to the cyberattacks conducted against selected Estonian private and public entities in 2007. During the 2008 Summit, NATO inaugurated its first Policy on Cyber Defence, aimed at protecting the Alliance's networks and defining requirements that the networks of its member states have to fulfil in order to ensure an appropriate collective cyber defence and crisis management capabilities.[54]

The 2014 Wales Summit marked a crucial development within the Alliance's work in the cyber domain, with the adoption of the Enhanced Policy on Cyber Defence. The policy called for a consolidation of the relationship between the Alliance and the industrial sector – implemented through the NATO Industry Cyber Partnership[55] – and more organised and timely information sharing and assistance among Allies. The Enhanced Policy also confirmed NATO's intention to uphold principles and norms of international law in cyberspace:[56] "NATO has made clear that a severe cyber attack could lead it to invoke Article 5 of the Washington Treaty".[57]

During the 2016 Warsaw Summit, the Alliance declared cyberspace an operational domain[58] and launched the Cyber Defence Pledge, namely an allied commitment

[54] Susan Davis, "NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence" (148 STC 19 E rev. 1), in *NATO Parliamentary Assembly STC General Reports*, October 2019, p. 1, https://www.nato-pa.int/node/56441. The Russia-Georgia conflict in 2008 proved the destructive power of cyberattacks. A team of Russian hackers conducted several cyberattacks against Georgian state and institutional websites, the Ministry of Foreign Affairs, the Ministry of Defence and the Presidency of the Republic included. These cyberattacks have been considered among the first cases of coordinated attacks conducted across different domains.

[55] NATO Communications and Information Agency (NCIA) website: *NATO Industry Cyber Partnership*, https://www.ncia.nato.int/business/partnerships.html.

[56] NATO, *NATO Cyber Defence Factsheet*, July 2016, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf.

[57] NATO, *The Secretary General's Annual Report 2020*, 16 March 2021, p. 23, https://www.nato.int/cps/en/natohq/opinions_182236.htm.

[58] NATO, *Warsaw Summit Communiqué*, 9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

to develop enhanced national cyber defence capabilities,[59] and a useful tool for an independent assessment of NATO's own progress in the cyber sector.[60] This decision followed a 60 per cent increase in cyberattacks against NATO infostructure if compared to 2015, with an average of almost 500 attacks per month.[61]

The following NATO Summit, held in Brussels in 2018, witnessed the inauguration of the CYOC, within the Allied Command Operation (ACO).[62] The CYOC is responsible for the Alliance's cyber activities: besides ensuring an adequate situational awareness of cyberspace, it is tasked with the planning of allied missions and operations and the management of possible operative issues.

The concept regulating allied operations in cyberspace is explained in the Allied Joint Doctrine for Cyberspace Operations, which was published early in 2020.[63] The document's objective is threefold: providing NATO staff with guidelines for conducting cyber operations; giving guidance to member states, partner countries, as well as other nations and organisation; and functioning as a reference point for civil and military entities within NATO.

Within the broader context of hybrid threats, often taking place in cyberspace, the Alliance developed a close cooperation with its partners – first and foremost the European Union, with which NATO collaborates in the fight against cyber threats.[64]

The Alliance's commitment to strengthening its cyber defence posture is also demonstrated by declarations released by its leaders. During the 2019 London Summit, NATO Secretary General Jens Stoltenberg defined cyberspace as a "new battleground".[65] The following year, NATO Deputy Secretary General Mircea Geoană stated it is not possible to "win and fight the wars and competitions of the future

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

[60] Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries: Comparing Models", in *IAI Papers*, No. 21|05 (February 2021), p. 8, https://www.iai.it/en/node/12727.

[61] NATO, *Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers*, 15 February 2017, https://www.nato.int/cps/fr/natohq/opinions_141109.htm.

[62] Laura Brent, "NATO's role in cyberspace", in *NATO Review*, 12 February 2019, https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

[63] NATO Standardization Office, *Allied Joint Doctrine for Cyberspace Operations* (AJP-3.20), January 2020, https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320.

[64] NATO website: *NATO's Response to Hybrid Threats*, last updated 16 March 2021, https://www.nato.int/cps/en/natohq/topics_156338.htm. The NATO–EU collaboration on cyber defence is mentioned in the Joint declaration on EU–NATO cooperation but also in the Technical Arrangement on Cyber Defence, both signed in 2016. See: Council of European Union, *NATO Summit, Warsaw, Poland, 8-9 July 2016*, 8 July 2016, http://europa.eu/!yw74vV; NATO, *NATO and the European Union Enhance Cyber Defence Cooperation*, 10 February 2016, https://www.nato.int/cps/en/natohq/news_127836.htm.

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

with the instruments of the past" and, in the context of the NATO Cyber Defence Pledge Conference 2021, he emphasised the Alliance's effort in the enhancement of its cyber resilience and its investments in new technologies, also through the collaboration with its partners.[66]

Such effort is included in the NATO 2030 initiative, aimed at a re-definition of the Alliance's agenda for the next decade and the development of a new strategic concept.[67] In this framework, the report elaborated by the Reflection Group – presented by Stoltenberg – asserted the importance of strengthening Allied cyber defence capabilities, improving NATO's recruitment, funding, and training procedures, and ensuring the Alliance can rely on legal and political structures able to respond to cyber threats.[68] The report highlighted the role played by the so-called emerging and disruptive technologies (EDTs) – also considering the race between China and Russia in this field – encouraging Allies to bolster their technological capabilities, especially in the realm of AI.[69]

For NATO to activate the collective defence clause, it obviously needs to identify the attacker. In cyberspace, as in other domains, the attribution of an offensive activity is crucial in order to implement an adequate response. Yet, such process is extremely complicated,[70] and continues to represent a serious challenge for the activation of the Alliance's collective defence.

3.2 Major NATO structures

In addition to the CYOC, which operated at operational level, the Cyber Defence Management Board (CDMB) within the Emerging Security Challenges Division works to prevent, manage and analyse cyber threats. The CDBM functions as a forum in which cyber defence specialists belonging to different NATO agencies can discuss the strategic planning and the executive direction of allied networks.

At the political and strategic level, the North Atlantic Council (NAC) – namely the entity responsible for the political decision-making process within the Alliance – is supported by the Cyber Defence Committee (CDC) in its cyber defence activities. In 2020, the NAC established that NATO was allowed to resort to instruments

[66] NATO, *Deputy Secretary General Mircea Geoană Said that NATO's DNA Is Values and Foresight*, 11 December 2020, https://www.nato.int/cps/en/natohq/news_180071.htm; NATO, *Deputy Secretary General Participates in NATO Cyber Defence Pledge Conference*, 15 April 2021, https://www.nato.int/cps/en/natohq/news_183128.htm.

[67] For further information, see NATO website: *NATO 2030*, https://www.nato.int/nato2030.

[68] Thomas de Maizière and A. Wess Mitchell (eds), *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.

[69] Ibid., p. 29-30; Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries", cit., p. 5.

[70] As previously underlined in detail in the Chapter 5.

belonging to any domain (not just cyberspace) to counter cyber threats.[71]

At a technical level, the NATO Cyber Security Centre (NCSC) and the NATO Computer Incident Response Capability (NCIRC) respectively work to prevent, detect and recover from cyberattacks, and safeguard allied networks through regular cyber threats analyses. Both agencies operate within the NATO Communications and Information Agency (NCIA), responsible for the procurement of capabilities essential to conduct cyber operations.

Finally, the Cooperative Cyber Defence Centre of Excellence (CCDCOE), based in Tallinn, plays a significant role in the study and analysis of cyber threats. The CCDCOE is currently finalising and promoting the third edition of the Tallinn Manual, which aims to offer an objective interpretation of the norms that could apply to cyberspace.[72]

Within the fast-paced context in which relevant NATO actors working in cyber defence operate, the CYOC could pave the way for the creation of a command for cyber operations, following the same scheme adopted for existing commands operating in the aerial, maritime and land domain.[73]

To ensure that all the aforementioned structures work in a complementary manner, with the ultimate goal of strengthening allied cyber defence, they need to implement a more efficient information sharing process. As a matter of fact such process is still lacking, complicated, and politically sensitive, much like in the intelligence sector.[74] To foster information sharing, mutual trust and national capabilities to counter cyber threats, in 2015 the CDMB was tasked to stipulate Memorandum of Understanding on Cyber Defence with national entities of each member states.

3.3 Activities with member states and partners

The Alliance conducts several educational activities on cyber defence and cybersecurity. For instance, in early 2021, the Rome-based Modelling & Simulation Centre of Excellence (MSCOE) organised a Cyber Wargaming course, and the NATO Rapid Deployable Corps Italy held a virtual conference on cyber operations and the security of critical infrastructure.[75]

[71] 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.

[72] CCDCOE website: *The Tallin Manual*, https://ccdcoe.org/research/tallinn-manual.

[73] Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries", cit., p. 6.

[74] Ibid., p. 7.

[75] Italian MoD, *NATO M&S COE: 1ª edizione del Corso Cyber Wargaming*, 22 January 2021, https://www.difesa.it/SMD_/Eventi/Pagine/NATO_M_S_COE_1_Edizione_del_Corso_Cyber_Wargaming.aspx; Italian MoD, *NATO: NRDC-ITA il Webinar sulle operazioni cibernetiche*, 9 March 2021, https://www.difesa.it/SMD_/Eventi/Pagine/NDRC_IT_webinar_sulle_operazioni_cibernetiche.aspx.

ISSN 2280-6164

Such commitment is also demonstrated by the collaboration between the Alliance, the private sector and academia. Against this backdrop, the NATO Allied Command Transformation (ACT) and the CCDCOE organised a workshop on the security of NATO's 5G military networks.[76]

NATO's work on cyber defence includes its cooperation with partner countries. For instance, in January 2021 the Alliance finalised a project aimed at reinforcing Mongolia's cyber defence capabilities,[77] and inaugurated a Cyber Response Capability Center in Moldova to enhance its armed forces' cyber defence competences.[78]

While demonstrating NATO's all-encompassing and cooperative cybersecurity approach to cybersecurity, Stoltenberg recently remarked the urgency to establish shared norms to ban offensive actions in cyberspace, promoting the idea to draft an international treaty regulating the cyber domain globally.[79]

3.4 The Italian effort

Italy participates in several initiatives aimed at strengthening the Alliance's cyber defence. For instance, NATO's Cyber Coalition exercise provides an opportunity in allied cyberspace defence training, also through simulations of cyberattacks against ICT networks and critical infrastructures.[80]

As a Sponsoring Nation, Italy supports the CCDOE – a valuable opportunity for international cooperation in the field of cyber defence, especially via two yearly exercises: the Crossed Swords[81] and the Locked Shields.[82]

Italy also has the opportunity to take part in initiatives organised by other Allies. For instance, the Cetatea exercise[83] organised by the Romanian Army aims at verifying the interoperability of communication and information systems of the participants.

[76] CCDCOE, *First Joint 5G Military Security Workshop Hosted by ACT and CCDCOE*, 5 February 2021, https://ccdcoe.org/news/2021/first-joint-5g-security-workshop-hosted-by-act-and-ccdcoe.

[77] NATO, *NATO Helps to Strengthen Mongolia's Cyber Defence Capacity*, 18 January 2021, https://www.nato.int/cps/en/natohq/news_180697.htm.

[78] Gregorio Baggiani, "The New NATO Cyber Incident Response Center in Moldova, in *NATO Defense College Foundation Articles*, 25 June 2021, https://www.natofoundation.org/?p=29468.

[79] NATO, *Speech by NATO Secretary General Jens Stoltenberg Followed with Questions and Answers at the 3rd German Ecumenical Church Days*, 15 May 2021, https://www.nato.int/cps/en/natohq/opinions_183679.htm.

[80] NATO ACT website: *Cyber Coalition*, https://www.act.nato.int/cyber-coalition.

[81] CCDCOE website: *Crossed Swords*, https://ccdcoe.org/exercises/crossed-swords.

[82] CCDCOE website: *Locked Shields*, https://ccdcoe.org/locked-shields.

[83] MSCOE website: *Exercise Cetatea 2019*, https://www.mscoe.org/?p=2514.

As discussed in Chapter 5, to ensure its full participation in allied operations in cyberspace, including activities and exercises encompassing offensive operations to counter cyber threats, the national legislation will need to allow Italy to take advantage of any and all possibilities the Alliance offers in this domain.

4. Cyber defence in major NATO states
by Ester Sabatino

In the major NATO states, cyber defence is implemented through national defence structures and strategies reflecting the state's approach to cyber threats. Although there is not just one single model for the organisation of the numerous cyber defence structures, it is possible to identify some similarities and differences among NATO countries[84] – particularly interesting when it comes to their position concerning the possibility to conduct offensive as well as defensive operations both to respond to an attack and to enforce "advance defence" and deterrence.

4.1 The United States

The United States (US) administration dedicates a lot of effort to countering cyber threats, both in operative terms and with the goal of shaping a common cyber defence doctrine at international level.

The entity responsible for national cyber defence is the US Cyber Command (CyberCom), which steers, harmonises and coordinates operations and planning in cyberspace, aiming to protect and promote national interests[85] through the achievement and retention of superiority in the cyber domain.[86] Working towards these objectives, CyberCom is supervised by the information system of the Department of Defence, with its Commander also holding the title of National Security Agency (NSA) Chief. Gathering representatives of the four military structures' cyber commands, the CyberCom supports each armed force as well as the Joint Forces Command through 133 operative groups formed in 2018, also as a result of a 600 million dollar investment.[87]

The cyber domain was once again recognised as strategic with the Interim National Security Strategic Guidance presented in March 2021 by President Joe Biden.[88] The current US administration considers cybersecurity one of its main priorities, and the development and reinforcement of cyber capabilities represent the cornerstone of its political agenda. Any response to a cyberattack is conducted in an active manner and follows the principle of advanced defence, namely a constant commitment in the cyber domain aimed at deflecting the adversary's abilities of

[84] For an overview of the main requirements common to the case study countries reported here, see Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries", cit.

[85] US Cyber Command website: *Our Mission and Vision*, https://www.cybercom.mil/About/Mission-and-Vision.

[86] 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.

[87] Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries", cit.

[88] US Presidency, *Interim National Security Strategic Guidance*, March 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/03/interim-national-securitystrategic-guidance.

both attack and defence with the ultimate goal of ensuring an operative edge.[89] Among its advanced defence activities, the CyberCom revealed it is conducting "advanced hunt" operations, also known as "hunt forward", namely actions aimed at gathering information on potential adversaries, sharing them with partners and Allies and ultimately harm or obstruct malicious cyber activities.[90]

Following the Colonial Pipeline ransomware attack in 2021,[91] the US President signed an executive order calling for higher cybersecurity standards also for private parties operating within the country. According to the executive order, federal agencies as well as their software suppliers will have to meet higher qualitative standards.[92] With this Presidential order, the US set the basis for the establishment of a Cyber Safety Review Board, namely a platform for public-private consultation through which, in the event of a serious cyberattack, it is possible to evaluate past strategies and elaborate the next steps. Enhancing the resilience of US technological infrastructures and systems will be the objective of a new public-private partnership which will encompass major national technological companies that have been investing to improve the security and resilience of their products.[93]

The role played by the US in conducting operations in cyberspace is particularly relevant, and the country may have a strong influence in the definition of shared norms at international level. The strategic guidelines presented by President Biden demonstrate the urgency to agree upon a set of principles for assessing the attribution of cyberattacks. Such assessment would allow to implement a proportionate response to the attack whilst abiding by international law. The Cyber Diplomacy Act 2021,[94] currently being discussed, prescribes the creation of a Bureau of International Cyberspace Policy, which would be tasked to advise the US State Department, within which it is set, on policies to be implemented in cyberspace as well as ongoing international diplomatic matters.

4.2 The United Kingdom

In 2020, the United Kingdom decided to take a clear stand about its role in the cyber domain at international level, inaugurating the National Cyber Force (NCF),

[89] US Cyber Command website: *Our History*, https://www.cybercom.mil/About/History.

[90] US Cyber Command Public Affairs, *US Cyber Command, DHS-CISA Release Russian Malware Samples Tied to SolarWinds Compromise*, 15 April 2021, https://www.cybercom.mil/Media/News/Article/2574011.

[91] Stephanie Kelly and Jessica Resnick-ault, "One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators", in *Reuters*, 9 June 2021, https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08.

[92] Gabriele Carrer, "Perimetro cyber, dopo l'Italia gli Usa. La rivoluzione targata Biden", in *Formiche.net*, 13 May 2021, https://formiche.net/?p=1388957.

[93] Andrea Shalal, "U.S. to Work with Big Tech, Finance Sector on New Cybersecurity Guidelines", in *Reuters*, 26 August 2021, https://www.reuters.com/world/us/cyber-threats-top-agenda-white-house-meeting-with-big-tech-finance-executives-2021-08-25.

[94] US Congress, *H.R.1251 - Cyber Diplomacy Act of 2021*, 23 February 2021, https://www.congress.gov/bill/117th-congress/house-bill/1251.

responsible for conducting also targeted offensive cyber operations.[95]

The Integrated Review of Security, Defence, Development and Foreign Policy, released in March 2021, disclosed the implementation of a new cyber strategy aimed at ensuring the UK is provided with any and all capabilities needed to detect, discourage and halt adversaries in this domain.[96] Although the strategy's update has not yet been disseminated, the Integrated Review offers several points for reflection. For instance, the document clearly refers to the possibility to employ cyber weapons – as well as any other weapon system[97] – to respond to an attack that would trigger NATO's Article 5, besides the possibility to resort to Active Cyber Defence (ACD) if needed.[98] Against this backdrop, the UK's "active defence" resembles the US' advanced defence.

Offensive cyber operations will be conducted by the NDF which, due to the high number of attacks perpetrated in cyberspace and given the need to implement a coordinated response, gathers personnel from the British MoD, the Government Communication Headquarters (GCHQ) and Intelligence services.[99] Because of the exacerbation of the cyber threat, since 2016 the UK has been increasing the amount of resources devoted to the cyber domain, and it created a 165 million pounds fund for innovation in the defence and cyber sectors for the 2016-2021 time period.[100] Another element demonstrating the UK's commitment to implementing a state-of-the-art cyber defence consists of a cyber corridor that was inaugurated in the North of the country – an association of both public and private actors working in the sector, which will favour the shaping of highly specialised professionals.[101] By doing so, London is attempting to implement the so-called "whole-of-society" approach prescribed by the Integrated Review, aiming to enhance national resilience and create public-private synergies, also by resorting to so-called "ethical

[95] London has launched a series of initiatives to increase the cyber resilience of its armed forces. One example is provided by the Land Cyber program, which aims to provide cyber protection for deployed personnel and equipment in areas with hostile electromagnetic fields. More information on the programme can be found here: UK Government, *Land Cyber Programme Guidance*, updated 23 February 2021, https://www.gov.uk/guidance/land-cyber-programme.

[96] UK Government, *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*, 16 March 2021, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

[97] Reference to other types of weapons was made to Trident nuclear submarines. See for example: Dan Sabbagh, Jessica Elgot and Patrick Wintour, "Defense Review: UK Could Use Trident to Counter Cyber-Attack", in *The Guardian*, 16 March, 2021, https://www.theguardian.com/p/gmkz7.

[98] For more information see: Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries", cit.

[99] UK Government, National Cyber Force Transforms Country's Cyber Capabilities to Protect UK, 19 November 2020, https://www.gov.uk/government/news/national-cyber-force-transforms-countrys-cyber-capabilities-to-protect-uk.

[100] Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries", cit.

[101] UK Government, *International Policy Review Puts Cyber at the Centre of the UK's Security*, 14 March 2021, https://www.gov.uk/government/news/international-policy-review-puts-cyber-at-the-centre-of-the-uks-security.

hackers" skilled in the identification of flaws within the system.[102]

4.3 France

In France, cyber defence is managed by the General Secretariat for Defence and National Security (*Secrétariat général de la défense et de la sécurité nationale*), which works in synergy with the National Agency for the Security of Information Systems (*Agence nationale de la sécurité des systèmes d'information* – ANSSI).[103] The ANSSI assigns the protection and defence from cyberattacks to two separate structures, coordinated by the Cyber crises coordination centre (*Centre de coordination des crises cyber*). The armed forces, together with the information system, guarantee offensive cyber missions and capabilities, whilst defensive missions and capabilities are the prerogative of the ANSSI.[104] The latter is supported by the Cyber defence command (*Commandement de la cyber défense*) which, besides being responsible for the cyber defence and cybersecurity of the French MoD's systems, infrastructures and operations, is required to intervene in the event of nation-scale cyberattacks.[105]

Following the cyberattacks perpetrated against two French hospitals,[106] in February 2021 French President Emmanuel Macron allocated 1 million euro to the enhancement of the country's security infrastructure.[107] Formerly, the 2019-2025 Military Planning Law prescribed an investment of another 1.6 million euro, as well as the hiring of 1,000 cyber combatants, aiming to reach 4,500 units in 2025.[108] Such funds were devolved in accordance with the plan for relaunch and investment planning, and is meant to demonstrate France's all-encompassing approach towards cyber defence. The new financial allocation will allow further investments in the research and development of secure-by-design technologies, which may be employed both in the public and private sector, and in the education and employment of more specialised personnel. To this end, in autumn 2021 a new cybersecurity campus will be inaugurated, functioning as headquarters of the major cybersecurity actors, and will allow the creation of synergies among parties

[102] UK MoD, *Ethical Hackers Collaborate with Defence to Strengthen Cyber Security*, 3 August 2021, https://www.gov.uk/government/news/ethical-hackers-collaborate-with-defence-to-strengthen-cyber-security.

[103] French Government, *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 »*, 8 July 2009, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020828212.

[104] 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.

[105] French Senate, *Délégation parlementaire au renseignement - Rapport d'activité 2019-2020 n. 506*, 11 June 2020, http://www.senat.fr/notice-rapport/2019/r19-506-notice.html.

[106] "Cyber Attacks Hit Two French Hospitals in One Week", in *France 24*, 16 February 2021, https://f24.my/7NQx.

[107] French Presidency, *Accélération de la stratégie nationale en matière de cybersécurité*, 18 February 2021, https://www.elysee.fr/emmanuel-macron/2021/02/18/strategie-nationale-cybersecurite.

[108] Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries", cit.

and improve their ability to react to cyberattacks.[109] Demonstrating France's serious interest in the cyber domain, the country retains 44 per cent of Campus Cyber.[110]

Inspired by the willingness to create shared norms at international level, in 2018 France launched the so-called Paris Call for Trust and Security in Cyberspace. In November 2021, during the Paris Peace Forum, France presented the results achieved so far throughout the working groups involved in the initiative.[111]

4.4 Germany

The year 2021 was intended to be particularly relevant for Germany's cyber defence, with the Cyber and Information Domain Service (*Kommando Cyber- und Informationsraum* – CIR) created in 2017 reaching its full operational capacity of 14,5000 units.[112] The CIR is considered equal to other armed forces' commands, representing the structure responsible for the security and integrity of the German MoD's ICT structures and weapon systems. In the event of an attack to the national cybersecurity system, the CIR supports the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – BSI), namely the national authority for cybersecurity.[113] Due to constitutional obligations, the CIR can only provide "administrative assistance" to everyday support activities. Should a large-scale cyberattack occur that demands the deployment of military staff, the personnel operating in the cyber domain requires preventive parliamentary authorisation, as in the case of the other armed forces.[114]

The year 2021 also witnessed the update of the 2016 Cybersecurity Strategy (*Cyber-Sicherheitsstrategie*).[115] Besides the amendments that were proposed,[116] the

[109] Campus Cyber website: https://campuscyber.fr.

[110] Campus Cyber, *Le Campus Cyber clôture sa 2ème augmentation de capital*, 28 July 2021, https://campuscyber.fr/?p=944.

[111] French Ministry of Foreign Affairs, *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, February 2021, 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.

[112] German MoD website: *FAQ: Cyber-Abwehr*, https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/cyber-abwehr.

[113] For more information on how the ICR acts in the national cybersecurity structure, see: national cyber security structure, see: Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries", cit., section 5.

[114] Ibid.

[115] German Ministry of the Interior, *Cyber Security Strategy for Germany 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.

[116] The Ministry of the Interior has presented key points that represent insights from which to elaborate possible further modifications: German Ministry of the Interior, *Eckpunkte für die CyberSicherheitsstrategie 2021*, March 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/03/eckpunkte-cyber-sicherheitsstrategie-2021.pdf. The key points were followed by the position of the Federal League of German Industry (*Bundesverband der Deutschen*

current defence structure should not experience major changes; yet, Germany is committed to improving the sharing of relevant information, both at national and international – EU and NATO – level, in order to improve its cyber resilience. Moreover, the country intends to define the types of operations that can be conducted as a response to a cyberattack.

The lack of an international regulatory framework outlining common norms and establishing a set of procedures to follow in the event of cyberattacks deeply affects Germany – not just on a normative level, but especially with respect to the possibility to respond and the possible ways of responding to a cyberattack. In order to bridge such a gap, in March 2021 the Federal Government published a position paper on the application of international law in cyberspace. The document determines that if state A perpetrates a cyberattack against state B causing physical consequences and damages to its territory, state A will have officially violated state B's territorial sovereignty.[117] However, the paper also dictates that a single attack against part of a critical infrastructure or aimed at causing malfunctions cannot be considered a violation of a state's territorial sovereignty, since there is still disagreement over the definition of the threshold for a cyberattack against a national entity. Germany emphasises the need for caution when implementing any counter-measure to a potential cyberattack, since they may have serious repercussions on other national sectors as well as society itself. In accordance with international law, Germany asserts its right to resort to any means for self-defence purposes, as long as the response is proportionate to the attack. Yet, this leaves room for debate in the so-called "necessity measures", namely active responses implemented due to a lack of options and as a response to attacks targeting an essential interest of the state. In such instances, the response to an attack can be enforced regardless of the damages it may cause, be they in the physical or cyber world.

4.5 Spain

In Spain, cyber defence is handled by the Joint Cyberspace Command (*Mando Conjunto del Ciber Espacio* – MCCE) created in 2020, supervised by the Chief of the Defence Staff. The MCCE is tasked with the management, control, coordination and execution of all the actions needed to preserve the armed forces' freedom of actions in cyberspace and the safeguard of national defence and security critical infrastructures.[118]

The MCCE was established on the basis of the former Joint Cyber-Defence Command (*Mando Conjunto de Ciberdefensa* – MCCD) and the Directorate

Industrie – BDI), *Cyber-Sicherheitsstrategie 2021*, 14 April 2021, https://bdi.eu/publikation/news/cyber-sicherheitsstrategie-2021.

[117] German Government, *On the Application of International Law in Cyberspace. Position Paper*, March 2021, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

[118] Spanish MoD, *Orden DEF/710/2020, de 27 de julio, por la que se desarrolla la organización básica del Estado Mayor de la Defensa*, Article 9, https://www.boe.es/eli/es/o/2020/07/27/def710.

of Information Systems and Telecommunications (*Jefatura de Sistemas de Información y Telecomunicaciones* – JCISFAS), no longer included in the structure of the Chief of the Defence Staff.[119] Within the MCCE operates also the team responsible for the response to IT emergencies in the military sector (*Centro de Respuesta ante Incidentes del Ministerio de Defensa* – Esp-Cert-Def), which cooperates with other national civilian CERTs.[120]

From an operative perspective, if necessary, the entity that should respond to a cyberattack is the (F*uerza de Operaciones en el Ciberespacio* – FOCE),[121] namely the only structure within the MCCE operating in a continuous and permanent manner in order to provide the best possible situational awareness.[122] In the event of an attack, the 2019 National Cybersecurity Strategy (*Estrategia Nacional de Ciberseguridad*) includes both defensive operations and responses meant to neutralise an attack though offensive actions deemed proportionate to the attack itself. However, differently from other allied countries, Spain does not allow offensive operations unless there is evidence of an armed assault.

The establishment of the MCCE can be considered a reaction to a cyberattack perpetrated against the Spanish MoD in 2019.[123] Following the attack, Spain released an update of its national strategy, with a new focus on the education of the personnel working in public administration, and asserted its intention to further update the document throughout 2021.[124]

Spain's cybersecurity policy assigns a significant role to public-private cooperation and, in an attempt to improve such collaboration, a National Cybersecurity Forum (*Foro Nacional de Ciberseguridad*) was inaugurated in July 2020.[125] The Forum is intended for the analysis of national technical capabilities which may be used and enhanced to meet the armed forces' needs.

[119] Spanish MoD website: *Mando Conjunto del Ciberespacio*, https://emad.defensa.gob.es/unidades/mcce.

[120] Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries", cit., p. 24.

[121] Spanish MoD, *Orden DEF/710/2020, de 27 de julio*, cit., para. 7.

[122] DefensaCom, *Nuestra Ciberseguridad, un bien estratégico* (video), 28 April 2022, https://youtu.be/o-GfMHdUrqI.

[123] 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.

[124] Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries", cit., p. 23.

[125] Foro nacional de Ciberseguridad website: https://foronacionalciberseguridad.es.

5. Cyber defence: Defending what cannot be defended

by Alessandro Marrone[126]

Cyberspace is a *sui generis* domain, with only some of the elements appropriate for other domains – all of which have a physical dimension – applying to it. Therefore, the cyber domain presents new challenges that require armed forces to be creative and adaptable, especially for Italy which, being a "middle power", does not have full control over an operative environment that is so difficult to defend.

5.1 Peacetime war and the cyber crisis

For years, cyberspace has been affected by a so-called "peacetime war".[127] That means that a confrontation among states is not officially declared, and there are no violent escalations which may lead to conventional war. Still, opponents invest significant resources to harm their adversaries' social and governmental structures and/or to test their vulnerability. Such resources are meant to support activities ranging from espionage, to Distributed Denial of Service (DDoS), to interference in political processes, to ransomware of data or critical infrastructures – as in the case of the attack to the US-based software provider Kaseya in July 2021, or the attack against the Lazio Region in August of the same year.

There are several similarities between cyberspace and the post-Cold War world, when several military operations were initiated without any official declaration of war, even in the case of high-intensity large-scale conflicts. This became especially frequent in the aftermath of the attacks perpetrated on September 11th, 2001. Nowadays, cyberspace is considered one of the domains where hybrid war is conducted, by resorting indiscriminately to any available resource at state's disposal.[128] Such phenomenon materialised in the resort to special forces, conventional military operations, all the way to the Russian occupation of Crimea in 2014.

Yet, the cyber domain poses one additional challenge. Whilst the political-military process of major NATO Allies – as well as the Alliance as a whole – has had to deal with both counter-terrorism operations and military activities against Russia, this has not been the case for significant cyber crises which, thankfully, have not yet been recorded. Therefore, it is not clear how NATO would react to such an occurrence, nor whether Article 5 of the Washington Treaty would be activated. It is

[126] The author is grateful to Vincenzo Camporini for his feedback on the first draft of this chapter.

[127] On the "peacetime war" concept, see: 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.

[128] See in this regard, among others: Hanna Smith, "Hybrid Threats to Allied Decision-Making", in Sonia Lucarelli, Alessandro Marrone and Francesco N. Moro (eds), *NATO Decision-Making in the Age of Big Data and Artificial Intelligence*, Brussels, NATO, March 2021, p. 44-56, https://www.iai.it/en/node/12844.

ISSN 2280-6164

not easy to evaluate the efficacy and efficiency of the current Italian and European governance in the identification of a potential attack, its timely and coordinated response, its ability to mitigate damages to data and critical infrastructure, to implement correct attribution, and to enforce all possible necessary actions in the defence-offence continuum.

5.2 Advanced defence of a space without boundaries

Because of the lack of tangible boundaries, the cyber domain resembles in some ways the maritime domain: theoretically, and with the exception of closed seas, every harbour on Earth is connected. Yet, there are three main differences between the cyber and the maritime domain. First of all, in cyberspace any route can be travelled in a split second, therefore there is no physical distance that could facilitate defence operations. Moreover, whilst it is possible to monitor the movement of opponents' fleets in the sea, cyberspace presents no such option, thus leaving room for a potential element of surprise favouring the attacker. Lastly, whilst an attack conducted from sea can only reach a country's coastal area, a cyberattack could hit any national asset, due to the current level of interconnection.

Given the elements characterising the cyber domain, by merely responding to cyberattacks a state systematically gives ground to its opponents, degrades its military power, jeopardises its IT systems, and encourages hostile powers to perpetrate increasingly sophisticated attacks – and this is especially true for major powers.[129] Metaphorically, it would be as if during the Cold War the US Navy had remained in American harbours, waiting for Russian ships and submarines to come, rather than actively patrolling the Atlantic and the Pacific to unveil their routes and hinder opponents' activities.[130]

For all these reasons, the current US CyberCom strategy mentions the concept of "advanced defence", which the US has traditionally applied to traditional domains, especially the aerial and maritime ones, and is now committed to implement in cyberspace, too.[131] By doing so, the US aims to "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."[132] The US intends to attain such superiority by enforcing "persistence" in operations, keeping the attention high through a well-structured campaign, continuously engaging with opponents and spreading uncertainty about the goals they mean to achieve. In other words, the US aims to attain an offensive-defensive

[129] Alessandro Marrone and Ester Sabatino, "Cyber Defence in NATO Countries", cit., p. 10-11.

[130] 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.

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

[132] US Cyber Command, *Achieve and Maintain Cyberspace Superiority*, cit., p. 5.

continuum of actions, operating as close as possible to its enemies, relentlessly trying to prevent them from gaining any operative edge and granting one to the US forces.[133]

The US has an unprecedented advantage in terms of human, economic, civilian and military resources, and thanks to the relevance of large US private companies in parts production, system integration, and data and network management. Nevertheless, both China and Russia – namely the most active powers in the cyber domain – as well as NATO Allies like France and the UK, Israel, and other smaller countries, adopt a similar approach, based on an uninterrupted sequence of integrated defensive and offensive actions. Such actions encompass threat intelligence,[134] monitoring, Advanced Persistent Threat (APT),[135] and reverse engineering activities – the latter target software, firmware[136] and hardware aiming to indirectly acquire competences and technologies needed to reproduce them. All the aforementioned activities share a common ratio and, taken together, constitute advanced defence[137] – though with a certain ambiguity.

The same kind of ambiguity characterised Italy's decision to employ Tornado fighter-bombers as advanced defence in the NATO campaign in Kosovo in 1999, also as a way to overcome internal opposition against the country's operations in lack of an explicit approval on behalf of the United Nations (UN). With regard to the defensive-offensive operations continuum in cyberspace, despite recent developments, Italy is falling behind in terms of normative and strategic planning on cyber defence, with partial drawbacks on doctrinal, operational and technological progress in the field. For instance, the extent to which Computer Network Exploitation – namely the collection of information on a specific target obtained accessing its data without compromising its functions – is permitted is not yet clear.[138] Similarly to the physical domain, where Italy has a thirty-year long experience conducting military operations abroad also in the absence of a declared conflict, the country could conduct advanced defence operations also in cyberspace.[139]

[133] Ibid., p. 6.

[134] For further information, see chapter 2.

[135] For a broader analysis of APT, see the deterrence and attribution section of this chapter.

[136] The firmware is a software programme or a set of instructions that form part of an electronic device and allow it to communicate with a computer or with other electronic devices.

[137] In the specialist literature, is also used the term "proactive defence" to describe the forementioned term, even if proactive defence is only partially comparable with advanced defence. Due to analytical and expositive clarity reasons and in consideration of its relevance in other publication, the author chose the latter term.

[138] Interview, 27 May 2021.

[139] Interview, 4 June 2021.

5.3 An impenetrable virtual domain

The laws of physics have different applications in cyberspace if compared to other domains. Firstly, because the time factor has a different impact in the cyber domain, with operations taking place in the matter of seconds; secondly, because all actors operating in cyberspace work with infra- and infostructures characterised by their own, constantly evolving norms, without which the cyber domain itself would not exist. Leaving aside the Matrix picture trilogy,[140] actors controlling these assets in today's virtual world hold, in some way, the keys of cyber networks. Therefore, they monitor cyberspace and can intervene with a broad spectrum of operation promptly or preventively. Anything making the Internet feasible can, by default, be used to control the network – from Internet providers, to server and data centres, to system productors like rooters, modems and computers, to microprocessors, software and antiviruses.

The US is advantaged by the fact that major American companies such as Microsoft, Intel, Cisco, Google, Apple, Facebook and Amazon own these assets. Therefore, the US government enjoys a privileged position in terms of data access and may influence the very use of the network. Suffice to think that the huge amount of data exchanged between Internet protocol (IP) devices travels via a series of connections and is then sorted through switches in which manufacturing companies and service providers can integrate probes to detect, decrypt and facilitate the flow of data in cyberspace without sender and recipient noticing any data sharing with third parties is taking place.[141] It comes without surprise that Beijing – Washington's foremost systemic rival[142] – invested substantial resources in ICTs, telecommunication and cyberspace in general, including 5G technology. China aims to elude the US' strategic advantage in this domain and impose its own edge, with unavoidable consequences for countries that will resort to Chinese technology in cyberspace. This may lead to the systematic integration black boxes and backdoors in billions of systems worldwide without users even knowing.[143] Only a well-organised pool of professionals with an expertise in engineering and informatics would be able to disclose such complex and concealed elements – an asset that only a few major public or private entities are able to acquire and preserve over time.[144]

This dynamic strongly influences and limits the cyber defence capabilities of a country like Italy. On the one hand, the strategic advantage of the primary NATO Ally guarantees collective defence, deterrence and opposition to strategic rivals such

[140] The Matrix, 1999; The Matrix Reloaded, 2003; The Matrix Revolution, 2003.

[141] Interview, 27 May 2021.

[142] When it comes to China, the term "systemic rival" has been employed in different EU and NATO documents. To take a case in point, the term has been cited in the NATO expert group's report launched by the NATO Secretary General Jens Stoltenberg in December 2020.

[143] Interview, 4 June 2021.

[144] Interview, 27 May 2021.

as Russia and China; on the other hand, this limits European strategic autonomy ambitions, especially in terms of contributions some member states could provide in filling technological gaps in the supply chain. More importantly, whilst the US and, possibly, China may to a certain extent influence the cyber domain, Italy does not have as much space for manoeuvre for its cyber activities.

Against this backdrop, strengthening the activities previously assigned to the CVCN as part of the National Cybersecurity Perimeter and now transferred to the ACN could be very significant for Italy's cyber defence. If conducted in a wisely, efficient and effective manner, through simple procedures and with appropriate resources, validation and certification activities may represent a first step for verifying and gaining a deeper understanding of ICT devices procured by public and private entities included in the Perimeter. By raising awareness on limits and vulnerabilities of the available tools, this process may lead to formulating an enhanced defence posture, identifying more reliable service providers and, possibly, supporting national providers on specific elements which could augment technological autonomy.

5.4 The deterrence and attack attribution problem

The cyber domain also poses new challenges to the principle of deterrence. There are two traditional ways in which it is possible to alter the enemy's strategic thinking and dissuade them from attacking: either deploying a defence line preventing the enemy from reaching their goal (deterrence by denial); or threatening a reprisal so severe that even a temporary victory would then turn into a ruinous defeat (deterrence by punishment). Against this backdrop, deterrence by denial cannot be implemented in cyberspace as building cyber defence capabilities is more expensive, complex, ineffective and inefficient than actually breaking through them, due to the offence-defence balance structurally leaning towards the former. Moreover, the speed governing technological progress might overcome cyber defence barriers so far deemed insurmountable. This does not mean one should not try to implement the best possible cyber defence: rather, it suggests employing any technological device and organisational procedure available useful for protecting against as many cyberattacks and actors as possible, limiting the chances of intrusion, damage and cyber crises to the best of one's abilities.

Yet, it should be noted that not even the most advanced cyber defence capabilities can withstand for an extended period of time a sophisticated, large-scale cyberattack perpetrated by groups of qualified people supported by a state actor with significant resources.[145] This is one of the reasons why France, the UK and the US decided to move forward with advanced defence, namely a continuum of counter-actions aimed at diminishing the opponent's offensive capabilities.

[145] Interview, 5 July 2021.

ISSN 2280-6164

Being aware of the fact that deterrence by denial cannot always work – especially against attacks conducted by state actors – both the US and NATO are working to implement deterrence by punishment. Recently, Washington tried to establish the difference between "destructive" attacks and "normal" online espionage activities, in an attempt to deter against the former and by suggesting tolerance towards the latter. The US also tried to distinguish between off-limits targets and targets that may be hit during conflict.[146] Against this backdrop, President Biden advanced a proposal to Russian President Vladimir Putin during the bilateral summit held in Geneva in June 2021. President Biden suggested including sixteen types of American critical infrastructures in the list of off-limits targets which may not be stroked by destructive cyberattacks, and discussing a similar approach for Russian targets. The underlying meaning of such a proposal was establishing red lines which should not be crossed in the cyber domain, whose trespassing may cause an escalation in other domains.

As discussed in the previous chapter, in the last few years also the Atlantic Alliance elaborated an official posture on cyber defence, claiming it is part of NATO's collective defence. In 2020, the NAC affirmed that Allies are determined not only to resort to cyber capabilities but also instruments belonging to the land, maritime or air domain to deter, defend from, or counter a cyberattack, thus suggesting a joint approach to all operational domains for NATO's deterrence and defence operations.[147] Such a strong declaration aimed at preventing cyberattacks so severe that could cause a conventional military response and which, so far, NATO has deliberately kept under the Article 5 threshold.[148]

The main issue with deterrence by punishment in the cyber domain, for all NATO Allies, concerns attribution. As a matter of fact, to ensure the response is directed towards the right actor it is necessary to identify the attack perpetrator, whilst holding enough evidence to publicly justify a potential reprisal. The lack of information and physical evidence, combined with the manoeuvrability of online data, makes attribution almost impossible to achieve.[149] It is however possible to acquire technological capabilities able to indicate the most likely source of an attack,[150] but it is then up to the political class to assign responsibility to an attacker and implement suitable deterrence and defence measures accordingly. Besides specific procedures at national level, establishing attribution is essentially

[146] Vladimir Soldatkin e Humeyra Pamuk, "Biden Tells Putin Certain Cyberattacks Should Be 'OffLimits'", in *Reuters*, 17 June 2021, https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16.

[147] Alessandro Marrone, "Nato e difesa cibernetica: una risposta militare ad attacchi cyber?", in *AffarInternazionali*, 22 March 2021, https://www.affarinternazionali.it/archivio-affarinternazionali/?p=87347.

[148] On NATO's role in peacetime warfare, see: 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.

[149] Interview, 27 May 2021.

[150] Ibid.

a political decision. What is more, the fact that different countries have different technological capabilities to verify attribution makes it difficult to have Allies agree over the authorship of the attacks. This implies that European states mostly have to trust the US' assessment in these situations.

In this framework, there has been an increased presence of APTs, namely cyberattacks in which the attacker penetrates a network without raising an alarm and is able to remain unidentified for a long time – possibly even months – continuing to intrude the network to achieve its goals. By analogy, the term APT has been associated with groups capable of carrying out similar attacks in an increasingly sophisticated manner, on a large scale and under cover, either autonomously or on behalf of the highest bidder, or even in the framework of more or less indirect relationships with states such as China, Iran, North Korea and Russia. Also, thanks to APTs, weapons meant for cyber warfare can be purchased online, and represent an extremely lucrative sector attracting groups of hackers that are becoming increasingly more organised.[151] Washington's repeated accusations against Moscow and Beijing – in the former case, with several NATO countries supporting the US – reflect this situation, which clearly facilitates anyone intending to hide the authorship of an attack.

In the context of the blurred virtual boundary between deterrence and defence it is now widespread the practice of hack-back, namely a counter-attack against the source that is believed to have conducted an attack, deemed proportional to the attack itself. Despite the aforementioned problem of attribution, different states – including NATO Allies – have different interpretations of the extent to which it is possible to consider an attribution certain and a hack-back proportionate to a given attack.[152] Still, it is crucial for states to obtain all the necessary tools to conduct such operations within the framework of the aforementioned advanced defence. In this respect, APTs are part of the problem as well as potentially part of the solution: since it is difficult to reconduct them to their sponsor states, they can be the target of hack-back operations that officially do not affect any third state, and are proportional to the attack received. Like Cold War mercenaries, and contractors in more recent times, APTs seem to be among the assets which, if sacrificed during cyber warfare, would not lead to further escalation.

Despite recent developments, this is yet another area in which Italy continues to fall behind other countries in terms of normative measures, thus preventing cyber defence authorities – and the COR in particular – from implementing much needed doctrinal, operational and technological developments. For instance, in the absence of a functional guarantee defined by the competent institutions, in a situation deemed legally non-confrontational the MoD may encounter problems in striking threats even if identified in due time.[153] Moreover, in the

[151] Ibid.

[152] Ibid.

[153] Ibid.

event NATO decided to implement a collective response to a cyberattack that hit one of the Allies, Italy would have to face regulatory obstacles contributing to the joint operational effort, as per Article 5 of the Washington Treaty. At tactical and operational level, Italy made progress on various fronts; yet, the overall situation is still unsatisfactory when compared to similar European countries such as France and Great Britain, which are much more inclined to hack-back or implement other forms of advanced defence.

5.5 Defence and resilience of the caste

Cyberspace is the realm of intelligence, covert operations, surprise attacks, fast and agile forces, and front overturns – elements that can be traced back to an Eastern approach to the art of warfare preached by Sun Tzu. It is therefore no coincidence that China seems very comfortable operating in this domain. Cyberspace is also the domain in which the eternal global race between attack and defence tools, from guns to shields onwards, accelerates at an exponential rate, quickly losing technological advantages that were obtained with difficulty, especially on behalf of the MoD.

In this context, in addition to available technologies, the organisation of the space that needs defending is very important for cyber defence. In this regard, the land domain offers a good metaphor. Similarly, to geography, with its mountains and rivers, also Italy's cyberspace is designed and continuously developed by foreign actors. However, the decision on where to build a castle is up to those who have to defend themselves. They have to decide whether to build it on the valley floor or on top of a hill, how to build it, the number of gates to be installed, the kind of walls to set up, and so on. Out of metaphor, cyber defence requires gaining a clear vision of the structure on which all other elements are built, and consequently the development of systems, networks, software, applications and any other component contributing to defining the way in which a given company or institution finds its place in cyberspace. Currently, the role of ICTs designers and developers is as important as that of professionals responsible for defending the network, who often operate *ex post* to "strengthen" cyber defence – yet, the two figures are disconnected. That is why there is a need for a paradigm shift whereby security is considered among the fundamental elements in the designing process of any type of system, starting from the earliest stages, *ex ante*, following the secure-by-design principle.

For instance, procuring all systems and software from the same supplier creates homogeneity, thus facilitating a cyberattack once the external line of defence is crossed. *Vice versa*, an irregular network made of elements acquired from different suppliers creates by default barriers and filters to a possible incursion on behalf of an adversary even once the latter crosses the perimeter to be protected. It goes without saying that an increase in the number of suppliers leads to an increase in the number of systems black boxes and backdoors. Yet, also in this case, parcelling out limits the amount of data that is easy to obtain from each supplier that has internal access, and makes it more difficult to obtain an overview – which is much more valuable than a series of partial information. In other words, "the whole is greater than the sum of its parts". Another example of secure-by-design consists in the development of networks whose nodes do not all communicate with each other, but are rather characterised by different levels of protection and whose data are stored in a fragmented manner, ensuring the most valuable are well-hidden. Metaphorically, if an attacker was able to cross the moat and the gate of the castle would have to limit its raid to the warehouses, leaving behind valuable objects kept in fortified tower, far from the walls, where each room can only be accessed through one door which can only be opened with one key. Individuals interested in conducting cyberattacks are shifting their focus from systems to data – something which cyber defence should take this into serious consideration.[154]

On the demand side of ICT, the problem of integrating those who manage networks and those who defend them affects the very organisation of public actors, especially – but not only – in the defence realm. However, the supply side is not immune to this, since the private sector envisions different educational and professional courses for those designing systems and those in charge of their security, to the detriment of the secure-by-design principle.[155] In this regard, Italy has taken an important step forward on the demand side with the establishment of the COR, which centralised the management of the armed forces network and the conduct of cyber operations in a single joint command and control chain. Such good practice should serve as an example for a broader coordination within the concerned ministries, in the government and in the Perimeter, so as to increase the resilience of all actors involved, thus their chances of defence. Once again, there is a need for a paradigm shift, going from only intervening after a cyberattack – which is inevitably quite an ineffective technique – to systematically preventing its occurrence.

5.6 The human being as a valuable and vulnerable technology

Cyber defence obviously requires technology. However, despite the advancements made in the field of ICTs and those currently taking place in Big Data and artificial intelligence (AI), human resources continue to represent one of the most valuable and vulnerable elements.

In order to transform the large amount of data collected and correlated by software into useful knowledge for cyber defence purposes, it is necessary to rely on professional analysts. They need to be enough to form a cyber defence team active 24 hours a day, seven days a week, especially if larger operations are to be conducted in the framework of advanced defence.[156] Similarly to the private sector, public administration needs to guarantee the constant presence of professional technicians able to develop the different functional elements ensuring cyber

[154] Interview, 4 June, 2021.

[155] Interview, 5 July, 2021.

[156] Interview, 27 May, 2021.

defence and resilience.[157] On both fronts, the number of university graduates from Italian universities is absolutely insufficient.[158] Such shortage of supply – compared to national and global demand – makes human resources even more precious and disputed, as previously emphasised with respect to the COR's difficulties in acquiring and maintaining adequate personnel.

Human resources are not only valuable, but very vulnerable from several points of view. In the armed forces, a poor understanding of the risks posed by ICTs and by operations taking place in cyberspace, both by individuals and organised groups, leads to the creation of large breaches in cyber defence, sometimes also through trivial behaviours. Moreover, those with access to data and networks in various capacities are, in some way, the guardians of the castle. If guardians are not adequately selected, educated and controlled, their surveillance risks not being vigilant enough, possibly even allowing an attacker to penetrate through a well-constructed cyber defence system.

[157] Interview, 4 June, 2021.

[158] Interviews, 4 June, 27 May and 4 July 2021.

6. Systemic criticalities and recommendations

by Alessandro Marrone and Ester Sabatino

In the last few decades, cyber defence has become increasingly important due to the high number of attacks against private actors as well as public administration and Defence structures, both within the national territory and abroad. The attack against the Lazio Region in August 2021 represented a great wake-up call for the Italian public opinion, also because of its connection with the vaccination campaign against Covid-19.

Within the broader framework of cybersecurity, cyber defence is characterised by a series of specific and essential elements, from three points of view. Firstly, the cyber domain can be considered as a high-intensity battleground: despite no conflict having been declared so far, cyberspace is affected by numerous attacks, which are carried out by a wide range of state and non-state actors, and can potentially trigger NATO's collective defence clause with repercussions also in the "real world". In this field, large and medium-sized powers deploy both military and non-military resources for the strengthening of state defence policy.

Secondly, as a consequence, new commands, agencies and units within the MoDs of Allied countries as well as at NATO level are being established in cyberspace, with repercussions for doctrinal and operational developments analysed in the previous chapters.

Finally, cyber defence offers the opportunity for a new strategic reflection on the meaning of defending and attacking, as well as deterring an attack, both in this operational domain and in the other four pervaded by cyberspace. Such a reflection has important implications for national security, structures and operations of the Italian Defence, the role of NATO, and Italy's position within the Atlantic Alliance.

Therefore, a focused analysis of cyber defence is needed to better address threats, risks and challenges, and to seize opportunities through mindful yet timely decisions, concrete actions and appropriate fundings.

6.1 The importance of a cooperative approach and an inter-sectoral dialogue

Acknowledging the peculiarity and importance of cyber defence does not imply compartmentalisation – quite the contrary. The variety of types of attacks and their possible repercussions calls for a cooperative approach among the various actors involved, as well as a comprehensive strategic reflection. This is especially true when considering that attacks targeting private actors of national importance or a critical infrastructure can have negative effects on national information and infrastructural systems with consequences both in the cyber domain and in the real world. Moreover, from the point of view of the MoD, every operational domain, besides cyberspace, can be hit by cyberattacks, both in Italy and abroad.

Concerning a possible cooperative approach aimed at achieving higher sectoral security standards, Italy initially demonstrated quite an innovative attitude in some respects, but then fell behind trying to keep up with the updates imposed by the speed of technological advancement and the pervasiveness of the cyber threat. As a matter of fact, while Italy's allies and partners at international level have long instituted agencies and structures connecting all the actors involved in the management and maintenance of national cyber security,[159] Italy only established the National Cybersecurity Agency in 2021.

The ACN is the primary actor in national cybersecurity. The decision to place the Agency directly under the Presidency of the Council of Ministers and outside the national intelligence system solves a series of former difficulties in management and operations. While the experience of the intelligence services' personnel remains unquestioned, the range of activities necessary to ensure cybersecurity goes beyond the ones specifically linked to this field. To this end, placing the ACN under the Presidency grants the President of the Council of Ministers – therefore the political leadership of the executive branch of the Government – the direction and control of the Agency.

The rationale behind this new legal and institutional framework, with special regard to the Perimeter and the ACN, consists in an inter-ministerial, collective approach on behalf of the executive branch and the public administration – each contributing according to their role – towards the issue of cybersecurity and cyber defence. Italy is in serious need of a similar approach for several aspects of national security, ranging from international missions abroad to defence exports,[160] from industrial policy[161] to critical infrastructures.[162] In the case of cyberspace, this is made even more urgent by the transversality of this domain.

Rationalising and reorganising national cybersecurity governance is a good investment for making the system more efficient. Yet, it will be important to take into account the specificities and competences of all the administrations involved, through an effort in coordination and collaboration at inter-ministerial level. Furthermore, given the pervasiveness of cyberattacks and their potential speed of action and penetration, it is crucial to rapidly examine all interests at stake, in order

[159] For example, in Germany the BSI was created in 1991 and France established the ANSSI in 2009.

[160] See in this regard: Alessandro Marrone, Michele Nones and Ester Sabatino, "La regolamentazione italiana degli accordi G2G nel settore della difesa", in *Documenti IAI*, No. 20|16 (September 2020), https://www.iai.it/en/node/12069; Alessandro Marrone, Ottavia Credi and Michele Nones, "Controllo parlamentare sull'esportazione dei sistemi d'arma: modelli comparati", in *Approfondimenti dell'Osservatorio di politica internazionale*, No. 180 (July 2021), https://www.iai.it/en/node/13826.

[161] Alessandro Marrone, "Politica industriale della difesa, se il ministro ci mette la faccia", in *AffarInternazionali*, 29 July 2021, https://www.affarinternazionali.it/archivio-affarinternazionali/?p=89012.

[162] See among others: Paola Tessari and Karolina Muti, *Strategic or Critical Infrastructures, a Way to Interfere in Europe: State of Play and Recommendations*, Brussels, European Parliament, July 2021, https://doi.org/10.2861/179721.

to promptly implement the most adequate response. This will happen through the intervention of the Cyber Security Unit, namely the body responsible for the response and management of cyber crises at a national level within the ACN.

During the phase of conversion into law of Decree-Law No. 82/2021, political decision-makers emphasised the role of the ministries involved in the national cybersecurity architecture – including the MoD – thus suggesting they recognised the importance of the dialogue between the various public and private actors. The ACN will have to consult the MoD when participating in projects and initiatives envisioning a collaboration with NATO and the EDA for the definition of aspects related to military research and the phase of sectoral training of personnel through the highly specialised competences of the armed forces.

A positive development in this regard could be a phase of collective training for officials of ministries and agencies who work – or will work in the future – in the field of cybersecurity, including military personnel. Just like the Joint Services Senior Staff College (*Istituto Superiore di Stato Maggiore Interforze* – ISSMI) represents an important step for strengthening the joint approach among the future leaders of the armed forces, a Cyber Defence Academy could represent an institute for advanced training where the experience gained in the defence sector could and should be matched with the competences provided by the public administration, aiming towards further cohesion within the Perimeter.

Moreover, the Parliament's decision to set up a Technical and Scientific Committee to support the ACN through proposals and consultations should be seen as a positive development. Having qualified representatives of industry, research institutions, academia and sector associations sitting around the same table with the Agency's personnel is a compelling attempt to enhance the dialogue among the actors involved, not only in order to coordinate the activities to be conducted, but also to evaluate the most appropriate ways to attain a higher level of cybersecurity.

6.2 Higher engagement of the industrial sector

In the cyber domain, it is important to always ensure an ongoing, systematic, multi-level dialogue between the MoD and national industry. Such a dialogue should envision a timely exchange of information on attacks occurring with increasing frequency and severity. Obviously, a similar exchange should ensure the highest level of confidentiality, involve and enrich all actors operating within the Perimeter, also in terms of increased defence and resilience against future attacks. The exchange should be two-way, with companies in the Perimeter that provide data on the one hand, and institutions which, in addition to collecting such data, should then appropriately share them to create greater shared situational awareness.

The dialogue on trends of cyber threats among the entities involved in the Perimeter is equally important, as well the one on technologies and related market trends. Involving the industrial sector in institutional consultation roundtables is particularly relevant in cyberspace, since those holding technological competences in the cyber domain also hold the cryptographic keys and the knowledge on their systems' functioning and on the large amount of data transmitted and exchanged on a daily basis. In IP-enabled devices, data travel through connections and are sorted through switches where probes can be specifically inserted to detect and decrypt relevant data, without sender and recipient realising that information is being shared with third parties. Since it would be unrealistic for the country to hold all the necessary skills to cover the entire technological chain required for a network ecosystem, to mitigate this problem Italy could aim to obtain some produced domestically switches and/or software, to limit national dependence on foreign suppliers and increase national resilience capabilities.

Therefore, it is important to enhance the Italian industrial sector through two lines of action. Firstly, continuing to use the Golden Power, where necessary, to ensure maintenance of national technological sovereignty in niche sectors of national competence deemed attractive to foreign investors. Besides safeguarding against inappropriate – if not hostile – foreign purchase attempts, Italy could be more active in identifying and enhancing the competences that may facilitate the creation of an autonomous national industrial and technological capacity. This may lead to the production of products, infrastructures, cyber and data management systems via a secure-by-design approach. Such a production would also contribute to the defence of the state. As a matter of fact, the first line of defence is provided by a high general level of resilience of state's products, infrastructures and systems. The decree converting Decree-Law 82/2021 into law emphasises the need to enhance cryptography as a cybersecurity tool and tasks the ACN with the qualification of cloud services. These two sectors, together with software and chip production – where national expertise can, in some cases, compete with foreign players – could be among the areas to be strengthened and supported by specific initiatives and investments. However, to ensure a functional application of the secure-by-design principle, the above-mentioned dialogue between the MoD and national industry is essential to create, maintain and develop a shared picture of national technological excellence in this field.

The first Directive on Defence Industrial Policy,[163] which was recently issued, highlights the need to establish a partnership between the MoD and national industry, and to direct attention and resources to industrial, technological and programme development capacities. A similar approach is especially important in the cyber sector which, counting for approximately 1.4 billion euro in Italy, is made of numerous small and medium-sized enterprises (SMEs) and start-ups that could increase the value of Italian competences in innovation and technology. The features characterising this sector, technology and the market lean towards fragmentation, dynamism and fluidity, thus making it difficult to achieve a public industrial policy. Nevertheless, an institutional effort is needed to ensure targeted,

[163] Italian MoD, *Direttiva per la politica industriale della Difesa, 2021 Edition*, https://www.difesa.it/Documents/Direttiva_Ministro_Guerini2907.pdf.

effective and efficient support, in the framework of a serious public-private partnership deemed necessary by several stakeholders, due to the strategic nature of the technologies at stake and the aggressiveness of international competitors and adversaries. In this context, priority attention should be given to start-ups and SMEs. Despite being bearers of potentially relevant technological innovation, if not adequately supported and integrated into an ecosystem of more established players, these actors risk being targeted by foreign investment aimed at seizing their skills and know-how.

Having taken these elements into consideration, and along the lines of other European countries, Italy could also create special economic zones where to base companies operating in the cyber domain. By doing so, such companies may adopt a systematic approach and support their work through different types of benefits and incentives. Technological advancement characterising the cyber sector takes place in a remarkably fast and uninterrupted manner, thus requiring consistent and targeted investments. Whilst making this effort, it will be important to take into account the advantages offered by the European Union through the Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF). The latter also provides the opportunity for financing and co-financing and, in this framework, special attention is drawn towards EDTs – including cyber applications – also in terms of European funding opportunities.[164]

6.3 Strengthening the joint approach and advanced defence

The adoption of state-of-the-art, secure-by-design systems, structures and software, whilst essential, is not sufficient to ensure defence, which must be enforced taking into account the pervasiveness of the threat, the types and intensity of cyberattacks, and their targets. The cyber domain requires a joint response, even more so than other operational domains, both to protect the networks of the MoD, and to be able to intervene in the civil-military continuum. As a matter of fact, both sectors are involved in cyberattacks, with special regard to civilian targets of strategic importance to the state.

Defence infrastructures, communication and information systems are protected by the COR, instituted in 2020 and operating with a joint approach. The Command's effort to work in this manner could be further improved, with positive effects on the concentration of demand, the elimination of inefficiencies and duplications, the exploitation of economies of scale and the increase in the interoperability of the systems employed, to be achieved through a process of integration of the operational aspects and technological developments. A similar process would benefit both public institutions and Italian industries working in this sector.

[164] On EDTs and EU initiatives see: Ester Sabatino and Alessandro Marrone, "Emerging Disruptive Technologies: The Achilles' Heel for EU Strategic Autonomy?", in *IAI Commentaries*, No. 21|31 (June 2021), https://www.iai.it/en/node/13569.

With respect to the operations that may be conducted in accordance with the Italian normative framework, the armed forces' approach is different from that of the major actors within the Atlantic Alliance. When comparing Italy's operations with those conducted in France, the UK, and the US, Italy stands out for making it impossible to carry out strictly offensive operations in the absence of an explicit attack. The COR benefits from a certain advantage in terms of maintaining the initiative over its adversaries when conducting operations, both within national territory and abroad. Yet, the "advanced defence" approach pursued by other NATO countries in various ways is not currently contemplated in Italy. Advanced defence brings advantages in terms of deterrence and resilience. However, to achieve such advantages it is necessary to adhere to a few rules of engagement deemed more flexible, as they authorise the armed forces to use and manage cyber countermeasures in response to a cyberattack on critical infrastructures.

The tools used to carry out a cyberattack are almost the same as those employed for peaceful uses of cyber networks, structures, systems and software. Therefore, the skills applied in the attack phase may also be employed to defend from and respond to hostile events. Similarly to the way in which a company may resort to reverse-engineering to acquire new skills and knowledge, being able to attack an adversary implies knowing the strategy that the latter will enforce for self-defence as well as the steps that will follow to complete the attack.

In general, the options and proposals described above, which Italy could implement to seriously address the issue of cyber defence, require higher, more definite and more consistent investments. The COR's delay in achieving its full operational capability suggests a need for greater investments in the cyber sector, especially in the training of highly qualified personnel that needs to be able to adequately respond to cyberattacks. The skills acquired by the armed forces could be gathered, standardised and employed for the training of civilian state officials involved in the broader framework of national cyber security, in line with the goal of rationalising actions and resources for the good of the national economic system.

6.4 Reflecting on NATO and the role of Italy

In conclusion, taking into consideration the global level and an historical perspective, it is possible to assert that NATO Allies in the 1990s and 2000s missed the opportunity to start a shared reflection on the implications of the Internet for international security. In a way, Russia and China understood such implications before the West, efficiently exploiting them over the past decade and forcing Allies to play a defensive role in this domain.

As pointed out in the previous chapter, thanks to the technological and economic supremacy of its high-tech and digital sector, the US is certainly in a privileged position to influence the cyber domain. However, American documents from the past few years suggest the US' concern about losing such an advantage to China, and about Russia's aggressiveness on online platforms in the framework of hybrid warfare.

In general, the lack of a common allied strategic reflection on this subject led to an impetuous technological and economic development, out of touch with national security priorities, which risks harming the secure-by-design principle that the West is currently trying to recover and implement.

Against this backdrop, in the past few years NATO has been preparing not only to operate in the cyber domain, but also to fully understand all its security implications. This also explains the Alliance's prioritisation of EDTs, many of which are intrinsically characterised by a cyber nature – starting with AI – and NATO's plea for international treaties regulating cyberspace. This ongoing reflection within NATO is relevant for Italy, and Rome should contribute by bringing its own take to the discussion.

Updated 27 September 2021

List of acronyms

ACD	Active Cyber Defence
ACN	Agenzia per la Cybersicurezza Nazionale
ACO	Allied Command Operation
ACT	Nato Allied Command Transformation
AI	Artificial Intelligence
AISE	Agenzia Informazioni e Sicurezza Esterna
AISI	Agenzia Informazioni e Sicurezza Interna
ANSSI	Agence nationale de la sécurité des systèmes d'information
APT	Advanced Persistent Threat
BDI	Bundesverband der Deutschen Industrie
BSI	Bundesamt für Sicherheit in der Informationstechnik
C4	command, control, communication and computers
C4D	Comando interforze C4 Difesa
CASMD	Concetto Strategico del Capo di Stato Maggiore della Difesa
CCDCOE	Cooperative Cyber Defence Center of Excellence
CDC	Cyber Defence Committee
CDMB	Cyber Defence Management Board
CERT	Computer Emergency Response Team
CIC	Comitato Interministeriale per la Cybersicurezza
CIOC	Comando Interforze per le Operazioni Cibernetiche
CIR	Kommando Cyber- und Informationsraum
CISR	Comitato Interministeriale per la Sicurezza della Repubblica
COC	Cellule Operative Cibernetiche
COFS	Comando interforze per le Operazioni delle Forze Speciali
COI	Comando Operativo di Vertice Interforze
COR	Comando per le Operazioni in Rete
CSIRT	Computer Security Incident Response Team
CVCN	Centro di Valutazione e Certificazione Nazionale
CyberCom	US Cyber Command
CYOC	Cyber Operation Command
DDoS	Distributed Denial of Service
DIFNET	Rete della Difesa
DIS	Dipartimento delle Informazioni per la Sicurezza
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPP	Documento programmatico pluriennale
EDA	European Defence Agency
EDF	European Defence Fund

EDT	Emerging and Disruptive Technologies
Esp-Cert-Def	Centro de Respuesta ante Incidentes del Ministerio de Defensa
FOC	Full Operational Capability
FOCE	Fuerza de Operaciones en el Ciber Espacio
GCHQ	Government Communication Headquarters
ICT	Information and Communications Technology
IOC	Infrastructure Operation Center
IP	Internet Protocol
ISSMI	Istituto Superiore di Stato Maggiore Interforze
IT	Information Technology
JCISFAS	Jefatura de Sistemas de Información y Telecomunicaciones
LADC	Laboratorio Addestrativo per la Difesa Cibernetica
MAN	Metropolitan Area Network
MCCD	Mando Conjunto de Ciberdefensa
MCCE	Mando Conjunto del Ciber Espacio
MoD	Ministry of Defence
MSCOE	Modelling & Simulation Centre of Excellence
NAC	North Atlantic Council
NCF	National Cyber Force
NCIA	NATO Communications and Information Agency
NCIRC	NATO Computer Incident Response Capability
NCSC	NATO Cyber Security Center
NOC	Network Operation Center
NSA	National security agency
NSC	Nucleo per la Sicurezza Cibernetica
PESCO	Permanent Structured Cooperation
PNRR	Piano Nazionale di Ripresa e Resilienza
RIFON	Rete Interforze in Fibra Ottica Nazionale
RNI	Rete Numerica Interforze
RSC	Reparto di Sicurezza Cibernetica
SIEM	Security Information and Event Management
SME	Small and Medium Enterprises
SOC	Security Operation Center
STELMILIT	Scuola Telecomunicazioni Forze Armate

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 6976831
iai@iai.it
www.iai.it

Latest DOCUMENTI IAI

Director: Alessandro Marrone (a.marrone@iai.it)

21 | 12en Alessandro Marrone, Ester Sabatino and Ottavia Credi, *Italy and Cyber Defence*

21 | 12 Alessandro Marrone, Ester Sabatino e Ottavia Credi, *L'Italia e la difesa cibernetica*

21 | 11en Ottavia Credi and Camilla Vianini, *Space and European Digital Sovereignty*

21 | 11 Ottavia Credi e Camilla Vianini, *Spazio e sovranità digitale europea*

21 | 10 Marietta S. König and Liliya Buhela, *The OSCE Asian Partnership: Developments and Thematic Priorities*

21 | 09 Ester Sabatino (a cura di), *La collaborazione italo-britannica nel settore della difesa e sicurezza dopo la Brexit*

21 | 08 Eleonora Poli e Margherita Salvia, *Unione europea: cittadinanza e beni comuni europei*

21 | 07 Valeria Branca, *Financing Infrastructure Investments for Local Communities*

21 | 06 Alessandro Marrone e Karolina Muti, *La difesa missilistica dell'Europa e l'Italia: capacità e cooperazione. Executive summary*

21 | 05 Alessandro Marrone and Karolina Muti (eds), *Europe's Missile Defence and Italy: Capabilities and Cooperation*