CYBER: A NEW DOMAIN FOR STABILITY POLICING?

Cyber: a new domain for stability policing ?

by Aldo Rosa

INTRODUCTION

At the NATO Warsaw Summit in July 2016, Allied Heads of State and Government recognised cyberspace as a domain of operations: it was a crucial step in recognising that NATO must defend itself as effectively as it does in the Air, on Land, at Sea and in the Space. It was at the same time a crucial step in elevating Cyber at the same level of the traditional threat (both conventional and nuclear) and requiring a significant shift in thinking about military operations. This also supported a relevant change from the previous idea of battlefield to a more evolved and comprehensive concept of battlespace. This article aims to provide a basic understanding of the Cyber Threat through some key definitions related to the actors and how they operate; how NATO is rapidly progressing to adapt to the new challenge; finally, it will spark some considerations more specifically related to Cyber from a Stability Policing perspective.

THE CYBER THREAT FUNDAMENTALS

First and foremost, to prevent any conceptual misunderstanding, we should focus on some basic definitions related to Cyber in order to better define the threat and its specific environment. According to the NATO glossary, cyberspace is the global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data[1]. This completely supports the concept of a (virtual) space able to conduct a full spectrum of activities defined by the Alliance as cyberspace operations: actions in or through cyberspace intended to preserve own and friendly freedom of action in cyberspace and/or to create effects to achieve military objectives[2]. This immediately leads to a relevant consideration: cyberspace is not only computers. This is a full environment including networks, technology, and data (and the people behind all of this should be not discounted). Once defined the operating environment (or, more appropriately, the domain), the threat should be identified and defined. There does not exist a NATO agreed definition; however, one of the most common definitions of Cyber Threat is any circumstance or event with the potential to adversely impact organizational operations (including mission,

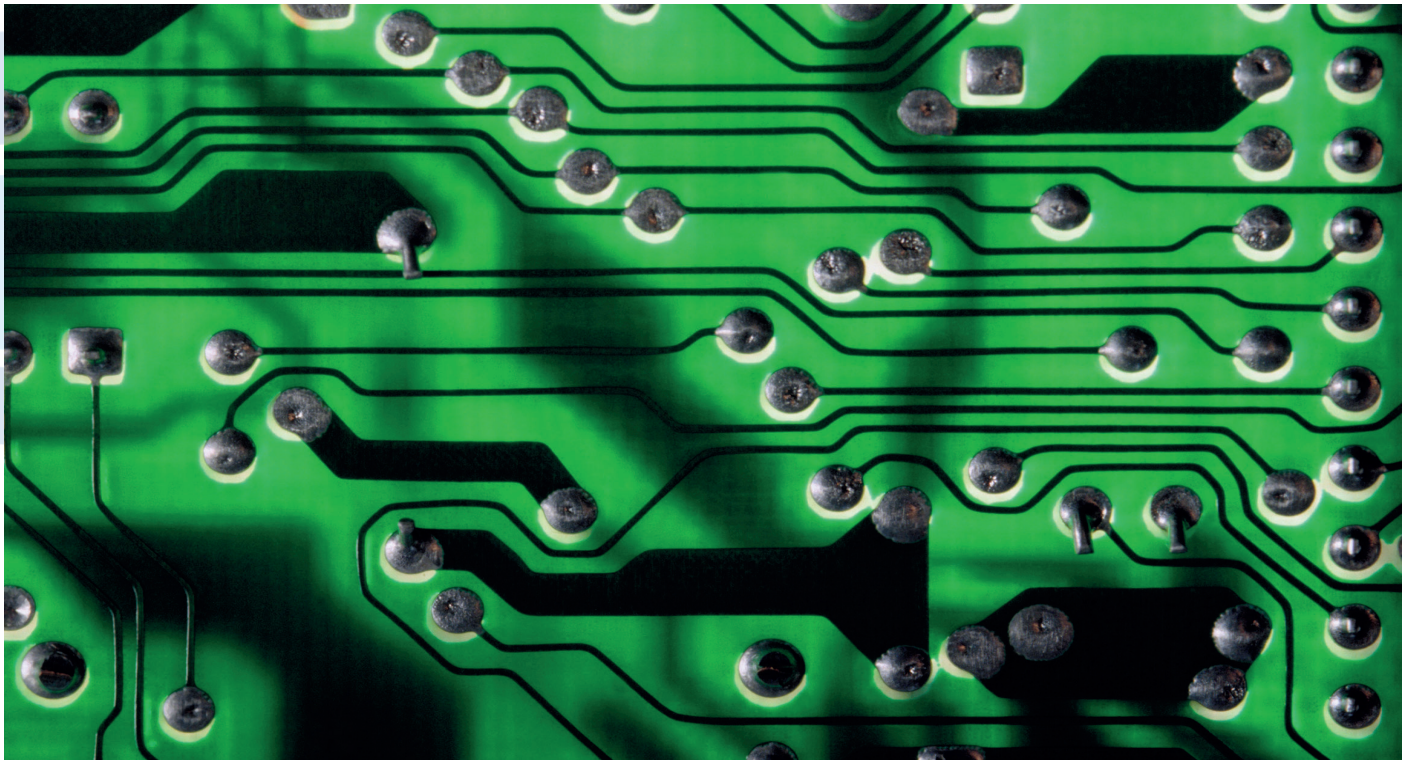
functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service[3]. The threat definition once again confirms that the Cyber perspective cannot be limited only to the "computers' world" and is required a new approach to military operations. A key factor of Cyber threat (and consequently of Cyber Operations) is represented by the virtual world: the absence of any "physical" boundaries is not supporting an easy distinction between what is the "military" part of the threat and the "civilian" portion of it, and elevating the Cyber Threat to the role of one of the most relevant ingredients of the Hybrid Threat. Erosion of distance, speed of interaction, low cost and difficulty of attribution are characteristics making the Cyber domain unique compared to the "traditional" domains[4]. As previously mentioned, Cyber is not only computers and the actors traditionally play a relevant role behind the threat itself. One of the most comprehensive definitions of Cyber actors is states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks. The globalized nature of the Internet allows these threat actors to be physically located anywhere in the world and still affect the security of information of the target system(s)[5]. Cyber threat actors have a different gradient of capability and sophistication and may operate on their own or as part of a larger organisation (notably state and state-sponsored groups or organised crime groups). From this perspective, sophisticated actors frequently put into practice any possible initiative in order to make it difficult for defenders to attribute the activity (so called obfuscation and false flag techniques)[6]. State and state-sponsored groups are generally considered to be the most sophisticated actors, with relevant resources and personnel, accurate planning and coordination and frequent links with private sector entities and organised crime groups (this is an additional factor in increasing the difficulties for attribution). One of the most complex, sophisticated and dangerous "structured" threat in use by state and state-sponsored actors is defined as Advanced Persistent Threat (APT): the most common definition of an APT is an adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives[7]. An excellent example about the complexity of an APT is offered by the model produced by Lockheed Martin and

> "ACCORDING TO THE NATO GLOSSARY, CYBERSPACE IS THE GLOBAL DOMAIN CONSISTING OF ALL INTERCONNECTED COMMUNICATION, INFORMATION TECHNOLOGY AND OTHER ELECTRONIC SYSTEMS, NETWORKS AND THEIR DATA, INCLUDING THOSE WHICH ARE SEPARATED OR INDEPENDENT, WHICH PROCESS, STORE OR TRANSMIT DATA"

defined The Cyber Kill Chain[8]: a seven-step approach clearly illustrating the need for the Adversary to put in place a sum of actions that requires a comprehensive approach not limited to the "computer world", as recently demonstrated by massive online foreign influence campaigns that seek to impact domestic events like an election, census, or public health. Finally, Cyber Threat actors can be categorised by their motivations and by their sophistication. In general, each type of Cyber Threat actor has a primary motivation: Nation state Cyber Threat actors are usually geopolitically motivated, Cybercriminals are generally financially motivated, and Hacktivists and Terrorist groups are often ideologically motivated.

NATO AND THE CYBER-DOMAIN

As a consequence of the cyber-attacks against Estonia's public and private institutions in 2007, NATO Defence Ministers agreed that urgent work was needed in this area. As a result, NATO approved its first Policy on Cyber Defence in January 2008. In the summer of the same year, the conflict between Russia and Georgia demonstrated that cyber-attacks have the potential to become a major component of conventional warfare. Since 2014 cyber defence has been recognised by NATO as an essential element of the Collective Defence[9] and NATO has affirmed the principle that international law applies in cyberspace as well. NATO's main focus in cyber defence is to protect its own networks (including operations and missions) and enhance resilience across the Alliance: at Warsaw NATO Summit in July 2016 cyberspace has been recognised as a domain of operations in which NATO must defend itself as effectively as it does in the Air, on Land, at Sea and in the Space. Following this crucial decision and recognising that cyber defence is as much about people as it is about technology, Allies also made a Cyber Defence Pledge in July 2016 to enhance their cyber defences, as a matter of priority. Since then, all Allies have upgraded their cyber defences and reinforced their capabilities for cyber education, training and exercises, including the creation of a dedicated Centre of Excellence, the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. Allies are committed to enhancing information-sharing and mutual assistance in preventing, mitigating, and recovering from cyber-attacks and since 2016 NATO and the European Union (EU) are cooperating through a Technical Arrangement on Cyber Defence. In the light of common challenges, NATO and the EU are strengthening their cooperation on cyber defence, notably in the areas of information exchange, training, research and exercises. At the same time, NATO is intensifying its cooperation with industry through a dedicated initiative, the NATO Industry Cyber Partnership (NICP). In 2018 a further crucial step was taken in setting up a new Cyberspace Operations Centre as part of NATO's strengthened Command Structure, making possible that NATO Cyber Rapid Reaction teams are on standby to assist Allies, 24 hours a day. The NATO Computer Incident Response Capability (NCIRC) based at SHAPE in Mons, Belgium, protects NATO's own networks by providing centralised and round-the-clock cyber defence support. This capability is expected to evolve on a continual basis and maintain pace with the rapidly changing threat and technology environment. In addition, NATO can now draw on national cyber capabilities for its missions and operations. In parallel, the appropriate doctrinal and legal framework has been established through several initiatives and a significant step forward has been taken at the Brussels Summit in June 2021, when the Alliance acknowledged the changing threat landscape, recognising that

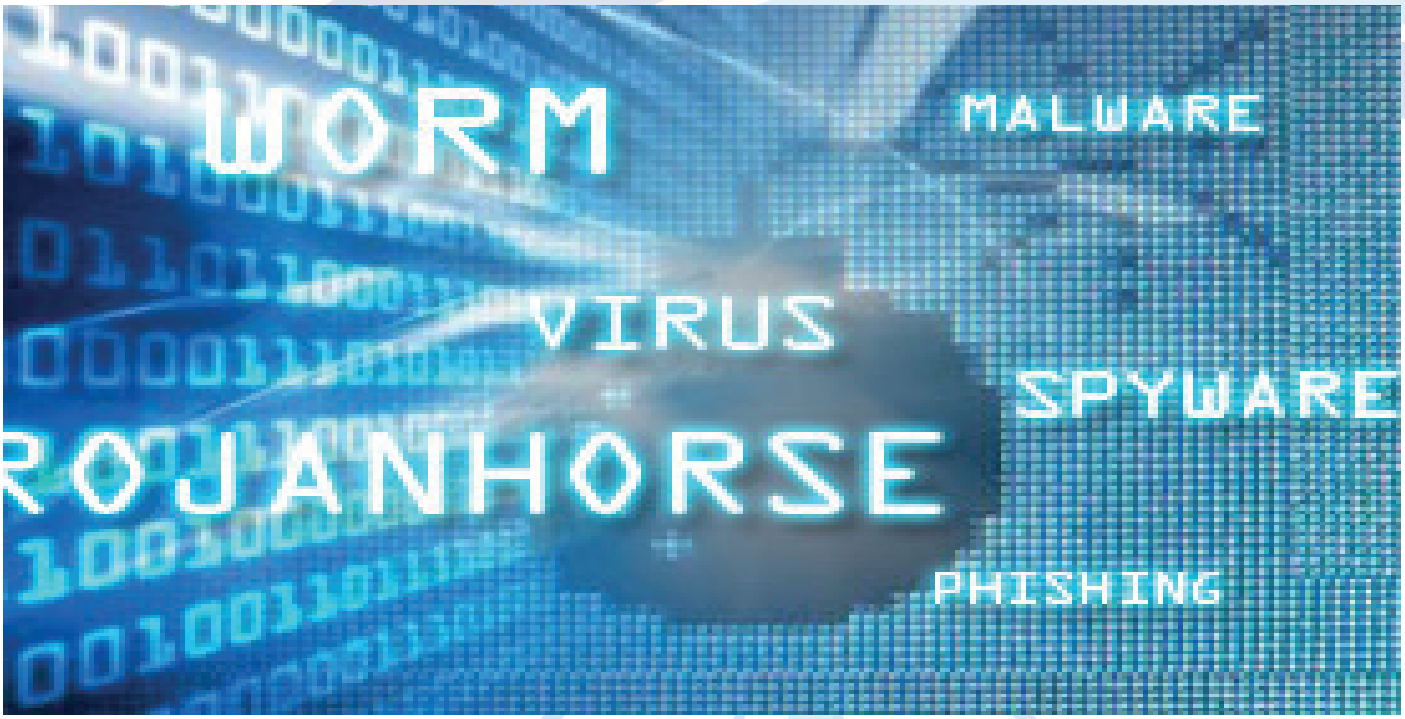


cyberspace is continually contested. In addition, Allies endorsed a new Comprehensive Cyber Defence Policy to support NATO's three Core Tasks mentioned before, as well as its overall deterrence and defence posture to further enhance the Alliance's resilience and making possible for Partner Nations to be constantly committed to employing the full range of capabilities to actively deter, defend against and counter the full spectrum of Cyber Threats. Cyber defence has also been integrated into NATO's Smart Defence initiatives. Smart Defence enables countries to work together to develop and maintain capabilities they could not afford to develop or procure alone, and to release resources for developing other capabilities. The Smart Defence projects in cyber defence currently include the Malware Information Sharing Platform (MISP) and the Smart Defence Multinational Cyber Defence Capability Development (MN CD2) project. Finally, from a comprehensive approach perspective, including the reinforcement of the international legal framework at the NATO Summit in June 2021, Allies reaffirmed their commitment to act in accordance with international law, including the UN Charter, international humanitarian law and international human rights law, in order to promote a free, open, peaceful and secure cyberspace and to further pursue efforts to enhance stability and reduce the risk of conflict. The evolving threat landscape, recognising that cyberspace is continually contested, requires a constant analysis of Cyber Threats, a close collaboration between incident response teams and the exchange of good practices concerning the cyber aspects and implications of crisis management. Since 2021 a new Comprehensive Cyber Defence Policy is supporting the above-mentioned NATO's three core tasks. According to expectations, the NATO Summit in June 2022 will be one more opportunity to reinforce the notion of Cyber as one of the major threats to the collective security and the new Strategic Concept will be possibly the opportunity to further consolidate Cyber as a priority.

> ALLIES ARE COMMITTED TO ENHANCING INFORMATION-SHARING AND MUTUAL ASSISTANCE IN PREVENTING, MITIGATING, AND RECOVERING FROM CYBER-ATTACKS AND SINCE 2016 NATO AND THE EUROPEAN UNION (EU) ARE COOPERATING THROUGH A TECHNICAL ARRANGEMENT ON CYBER DEFENCE

IS IT TIME TO THINK IN TERMS OF CYBER-STABILITY POLICING?
Traditionally considered part of the

Land Domain and conducted by Land-oriented forces, Stability Policing (SP) for NATO is defined as Police-related activities intended to reinforce or temporarily replace the indigenous police in order to contribute to the restoration and/or upholding of the public order and security, rule of law, and the protection of human rights.[10] In fact, the definition does not exclude at all any different approach required to include the Cyber Domain as part of the SP Battlespace and the existing NATO doctrinal framework does not close the door to cyber in Stability Policing. As briefly pointed out in the previous paragraphs some basic ingredients of the Cyber Threat perfectly fit the Stability Policing environment and are rapidly emerging as a reality that cannot be further ignored or under-estimated as part of the evolution of the Stability Policing vision and the related capabilities. More specifically, some considerations support the need to dedicate more attention to the Cyber Domain from the Stability Policing perspective: First: thinking only in terms of "computers" could be a critical error; Cyber is no longer an activity for "practitioners" and ignored by the rest of the Force. Commanders at any level should start thinking in terms of possibly conducting SP activities also in the Cyber Domain and they should be properly educated to do so by having Cyber as part of their basic set of skills. It is not only matter of giving them technical skills as they have to enter into a virtual dimension with no-boundaries and have the ability to rapidly shift from the traditional Land dimension to the virtual dimension of the Cyber Domain. Second: Cyber is at the same time a substantial ingredient of the Hybrid Threat. Both Cyber and Hybrid are characterised by the absence of physical borders (as previously pointed out), consequently there is very little (or no) distinction between a purely military context and a civilian environment, clearly creating a Safe And Secure Environment (SASE) and Freedom Of Movement (FOM) is a paramount in a SP mission: it is probably time to consider the option to think in term of a cyber-SASE and a cyber-FOM from the perspective of a comprehensive approach. Understanding the Operating Environment and Understanding the Threat are by doctrine[11] two essential elements of the Planning Considerations in support of a SP mission. Nowadays Cyber can be undoubtedly considered as a relevant part of the threat and an essential ingredient of the Operating Environment, therefore by syllogism Cyber cannot be ignored in a SP mission. Fourth: Law Enforcement (LE) has ting room for SP as one of the tools to effectively operate in a Joint, Inter-agency, Inter-governmental and Multinational response to the resolution of the complex challenges of a crisis offering innovative and scalable options by expanding the reach of the military instrument. Third: Establishing and maintai-



an important role to play in support of the Host Nation, particularly when it comes to domestic defensive cyber operations[12]: the frequent obfuscation of the adversary has relevant legal implications, potentially involving Host Nation's legal authorities, and States are called to seek additional innovative updates to laws that will allow LE to take appropriate measures. In addition, it should also be considered that SP Assets (when mandated) can conduct a LE activity in Cyber Domain as part of the Temporary Replacement mission within fragile states. Police Capacity Building is a key role to develop and improve the police capabilities in fragile states and SP can offer a relevant contribution also to deter the development within fragile states of cyber-sanctuaries having the ability to harm the security of the Alliance and its member states. Finally, there is a serious risk to have "Stone Age commanders" in a highly sophisticated operating environment and to face an evolved adversary putting in place an evolved threat if we do not rapidly change our mindset and expand the SP perspective as part of a comprehensive approach vision. Part of the solution could be the virtuous cycle sustained by NATO through CoE's systemic approach: the "past" properly processed by the Lessons Learned loop can generate useful inputs to be developed by the Concept Development & Experimentation Pillar, to be captured and consolidated through the Doctrine Development & Standards component, and finally transferred to the operational world by the Education and Training Pillar. A prompt change of mindset is required due to a big risk of being "left behind" by the rapid evolution of the threat; a significant effort should be made to constantly maintain the operational advantage against the enemy, thus avoiding a dangerous "chase the (cyber)-threat" approach. Cyber-instability is progressively becoming a reality: consequently, the need for cyber-stability cannot be ignored.

note

1 AAP-06 NATO Glossary of terms and definitions (ed. 2021)

2 AAP-06 NATO Glossary of terms and definitions (ed. 2021)

3 US National Institute of Standard and Technology (NIST) – Computer Security Resource Center (CSRC)

4 Joseph S. Nye Jr., The end of Cyber Anarchy. Foreign Affairs, Jan-Feb 2022

5 Canadian Centre for Cyber Security: An Introduction to the Cyber Threat Environment. https://cyber.gc.ca

6 Obfuscation refers to the tools and techniques that threat actors use to hide their identities, goals, techniques, and even their victims. In order to avoid leaving clues that defenders could use to attribute the activity, threat actors can use either common, readily available tools and techniques or custom-built tools that covertly send information over the Internet. (FireEye Cyebr Security at https://fireeye.com) Sophisticated threat actors can also use false flag, whereby an actor mimics the known activities of other actors with the hope of causing defenders to falsely attribute the activity to someone else. For example, a nation-state could use a tool believed to be used extensively by cybercriminals. (FireEye Cyebr Security at https://fireeye.com)

7 US National Institute of Standard and Technology (NIST) – Computer Security Resource Center (CSRC)

8 Lockheed Martin. Gaining the Advantage. Applying Cyber Kill Chain Methodology to Network Defense. 2015

9 Collective Defence, Crisis Management and Cooperative Security are the three Core Tasks identified by the NATO Strategic Concept adopted in 2010 at the Lisbon Summit.

10 AAP-06 NATO Glossary of terms and definitions (ed. 2021)

11 Allied Joint Publication AJP 3.22 - Allied Joint Doctrine for Stability Policing

12 America's Cyber-Reckoning. Sue Gordon and Eric Rosenbach – Foreign Affairs Jan. – Feb. 2022

PICTURES:
Aldo Rosa

Aldo Rosa
Lt. Col. – Italian Carabinieri
NATO Stability Policing COE
Acting ALS Section Chief /
Security Officer