er

verywhere apidly

Issue 31 - July 2021

DEEP WATCHING ON CYBER THREAT

NATO OTAN

NRDC - ITA

UBIQUE CELERE

The Magazine of the
NATO Rapid Deployable Corps - Italy

NATO Rapid Deployable Corps - Italy
Ubique Celere

CONTENTS

/NRDCItaly
@NRDCITA
NRDC ITA
NRDC-Italy

Everywhere Rapidly is the authorized official publication of the NATO Rapid Deployable Corps, Italy. All editorial content of Everywhere Rapidly is coordinated, for publication, by the Public Affairs Office.

Printed by: Grafica Olona

er Everywhere Rapidly

FOREWORD

In 2016, NATO recognized cyberspace as the 4th domain of warfare, extending "Article V" to cyber and further pledged to enhance the cyber defence of national networks and critical infrastructures as a matter of priority. Cyberspace activities have an increasing impact not only on the traditional physical domains of operations, but also on the political environment and public opinion, influencing national and collective decision makers. From a formal military perspective, Armed Forces throughout the world are elaborating a new approach on how to improve planning and execution of Multi Domain Operations, including Cyber and Space, against multi-dimensional objectives, ranging from physical, cognitive, and virtual.

Due to the swift evolving technological horizon, cyber defensive approach must be maintained at the state of the art, to cope with the whole range of potential cyber-attacks from State and non-state actors. As a consequence, the real question that we are called to address today is: "how emerging technologies, can contribute to improve Cyberspace Situational Awareness and Mission's Decision Making Process?". With this in mind, in March 2021 we have organised a CYBER WEBINAR at the NATO Rapid Deployable Corps – Italy, to share knowledge on "Cyberspace Operations in the Multi Domain approach and Security of Critical Infrastructures", held with the virtual presence of representatives from the NATO and National Command Structure, the Italian Information Security Department, Universities and Defence Industry.

This Edition of the ER magazine is dedicated to the outcomes and achievements of the Seminar, which offered the opportunity to elaborate on a series of stimulating and innovative topics that are at stake in the Alliance debate today. This goes in pair with Multi-Domain Operations, that represent an important challenge for NATO and the European Union, requiring not only a new approach in terms of planning and execution of operations but also on the procurement of advanced C2, intelligence and communication platforms. The success of future Multi-Domain Operations will depend, more than ever, on the capability to simultaneously direct tactical, operational and strategic assets, preserving the initiative and gaining momentum.

Malicious cyberspace operations could create a significant "short-term" effect on a targeted nation's economy, affecting also critical infrastructures. Even though every NATO nation could be able to manage these effects, it must be considered the overall corrosive effect against the Alliance's image and reputation. On the other hand, it is worth to consider that technological innovations, ranging from Artificial Intelligence to Quantum Computing, from 5G to virtualization of an increasing number of services, will be crucial for carrying out successfully missions along the whole spectrum.

In conclusion, it is important that NATO and the EU continue fostering multinational collaboration and involve industries and universities to exploit emerging technologies. Therefore, a continuous and deeper analysis should be collectively conducted on technology innovations to identify what capabilities need to be modernised and adapted in order to face future threats and challenges. In this context, the implementation of the Multi-Domain Operations concept implies the understanding of the related technical demands and policy implications, in order to offer NATO Alliance members appropriate solutions to obtain and maintain decisive advantages for future war fighting and deterrence.

INTRODUCTION

Military organization, Swiss precision, friendly welcome. The seminar on Cyberspace operations and security of critical infrastructures began under the best auspices at the NATO base in Solbiate Olona on 3 March. Introduced by General LTG Guglielmo Luigi Miglietta, NRDC-ITA Commander, it was the occasion to discuss the importance of protecting critical infrastructures. A clearer expression when we say that the infrastructures we are talking about are the transport, energy and people networks, hospitals and health facilities, but also banks and insurance companies, and that they are critical because their possible malfunction affects the proper functioning of all social activities for leisure, study and work.

Cyber attacks on critical infrastructure have increased over the years by rogue states and unscrupulous criminal gangs, sometimes as a side effect of digital robberies such as ransomware attacks that encrypt attacked computer systems and make them unusable until a ransom is paid. In Italy it happened to the detriment of a national electricity grid operator, but attacks of another nature had in the past caused renewed blackouts on large portions of European territory.

Questioning how to defend oneself in the face of such extreme scenarios is the task of everyone, including the Army and law enforcement agencies. Of course, the awareness of customers and employees who can open the door to the attacker unintentionally is important, but everyone has their own task to perform.

Is the world of national, European and NATO defense ready to respond to these challenges? Maybe yes, but without delusions. The enemy is treacherous, prepared and has the surprise factor on his side.

In addition, the now daily confrontation with sabotage and industrial political espionage actions make us understand that readiness is important (Ubique celere!) But that also the innovation of techniques, tactics and strategies must go hand in hand with the creation of technologies useful for combating cybercrime. It is a constant chase, cat and mouse, or if you prefer, with digital thieves and cybercriminals.

These digital thieves engaged in emptying bank accounts and extorting ransoms often operate in the service of rogue states for which they conduct offensive operations aimed at weakening opponents, with real campaigns of perception manipulation or through the theft of goods and compromise of services, to sow fear, doubt and uncertainty in a targeted population. The APTs themselves, the cyber paramilitary groups that conduct these operations, tend to repay their service with a percentage of the stolen goods from banking attacks or cryptocurrency laundering. There is an evident connection between the world of common criminals and state criminals, the nation-state hackers.

And precisely in this context, the pandemic scenario has catapulted us into a world where digital access and connectivity are no longer a choice, but a necessity to carry out many of the activities online we did in person before, physically present in designated places, schools, hospitals, offices, interacting with doctors, teachers and work colleagues. Protecting the networks on which these interactions are based is a vital issue that affects the quality of both our democracy and our economy.

We cannot afford to let our guard down. The NATO commaders I met are aware of this and are prepared for even the most catastrophic scenarios, but to put them in a position of advantage over spies and criminals, the intervention of politics is very important, which must take full responsibility for them without delegating the choices they make to technicians. The Tallin Manual may not be sufficient for the next crisis and we will need to know if it will be possible to react, and fight back with adequate tools. The answer concern the safety and well-being of all of us.

Greetings, NATO! Be beady to hack back!

About the Author

Former Director of Communication of the National Cybersecurity Lab (CINI) Professor Arturo DI CORINTO is now senior associate at CCSIRS - Center for Cyber Security and International Relations Studies, university of Florence and has experience as a **psychology researcher and professor** at the Stanford University (CA), Carrara Academy of Fine Arts, Link Campus University, and Sapienza University of Rome, where he currently teaches "Digital identity, privacy and cybersecurity" in the faculty of Political, Social and Communication sciences. He also served the Presidency of the Council of Ministers as an expert in public communication. Technology journalist, he wrote for Il Sole 24 Ore, La Repubblica, Wired and L'Espresso. He has also published several books and 2.200 article covering topics such as Internet governance, copyright, encryption, privacy and cybersecurity.

A Perspective on the future of Cyberspace Operations

Lt Gen **Richard CRIPWELL**, British Army

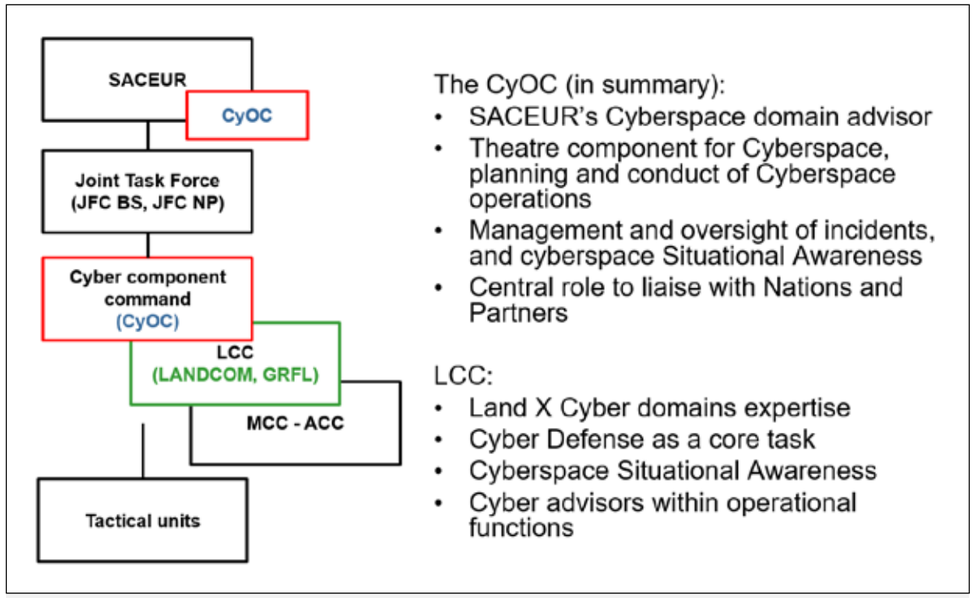
In December 2020, FireEye made public one of the most severe cyber attack ever conducted. In compromising updates for a Solar Winds software, an actor gained access to approximately 18,000 clients' Information Technology (IT) systems around the world, to include some of the most powerful commercial companies and most vital public institutions. The attack, extremely complex, leaves no doubt only a state actor has conducted it: evidence that cyberspace is a domain more and more governments are choosing for confrontation and competition.

Recognizing Cyberspace as a domain of operations

For many years, most actors (governments, international organizations, or industries) have just considered "cyber" as the technical way to protect their IT systems. With a burst of cyber attacks, they cannot continue to conform to a "cyber-defense only" posture. Based on strong Communication and Information Systems security, it is timely to concretely integrate cyberspace operations into the conduct of all aspects of operations. At the 2016 Warsaw Summit, NATO officially recognized cyberspace as a domain of operations:

"[We] recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances." (Warsaw Summit Communique – 9 July 2016)

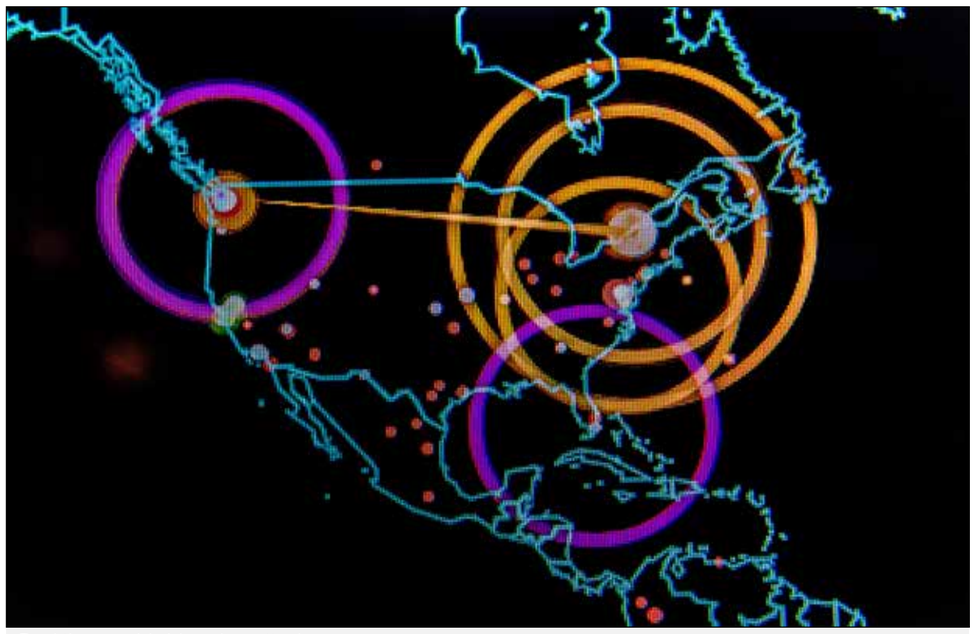
Satellite dishes for Telecommunications



An Example of Cyber C2 chain of command

A clear and simple doctrine for cyberspace operations

Defending an IT system is not something new but operating in a relatively new and complex domain such as cyberspace is a different challenge. As ever with the creation of an entire capability, NATO's primary focus is to define a common reference baseline of policies, doctrines, and standards. Issued in January 2020, the *Allied Joint Publication 3.20 – doctrine for cyberspace operations* is a must-read reference. In genuinely considering cyberspace as a domain and not a function, it adapts the *Allied Joint Publication 3 - doctrine for the conduct of operations* to the domain specificities. It encourages a military commander to apply the traditional principles of operations they already know and to seek the same effects from and in the cyber domain, that they would expect from other operational functions in the physical domain.


Real time worldwide cyber attack screen

Enabling the development of the capability

Since the recognition of cyberspace as a domain of operations, NATO makes progress in showing its willingness to "deter, defend and counter the full spectrum of cyber threats" by integrating a "full range of effects". Augmenting the command structure with new cyber positions in the face the actual threats and creating the Cyberspace Operation Center (CyOC), NATO has defined the missing pieces for a domain command and control structure. NATO is also providing the complete environment to build and grow its own capability as well as supporting the alliance members and partners doing so. Despite a challenging COVID situation, NATO has readjusted its training capabilities in a very reactive way. NATO training centers are proposing many distance learning solutions to maintain an education capacity for highly skilled specialists. NATO commands and the Collaborative Cyber Defense Center of Excellence (CCDCOE) Tallinn are also continuing to organize some of the largest cyber exercises in the world (-eg., Locked Shields, Cyber Coalition) demonstrating how NATO, NATO nations and partners can effectively interoperate in the domain.

Cyberspace and deterrence

Creating and demonstrating a capability to conduct operations and to create effects in cyberspace fundamentally contributes to deterrence. Cyber defense is the part of cyberspace operations contributing to deny an enemy to attack. NATO, in its ability to defend its network and make it resilient, to define high security standards for all the Allies and in its strength to communicate information and coordinate actions towards members and partners, is making clear it would cost more for an enemy to attack than the gain they would make.

In addition, NATO is working with 9 member nations to develop offensive cyberspace operations: the SCEPVA framework – Sovereign Cyber Effect Provided Voluntarily by Allies. Even before recognizing cyberspace as an operational domain, NATO confirmed at the 2014 Wales Summit that international law applies in cyberspace and that cyber defense is a part of the Alliance's core task of collective defense. A cyber attack might be considered sufficient for an Article 5 declaration. Further, NATO already has the legal framework and the operational process (targeting) to allow either a non-lethal or kinetic reaction.
In a very short time, NATO has adapted its policy and structure to face actual threats. The environment to integrate cyberspace operations into modern warfare is now established. NATO, with allies and partners are strong together to deter adversaries in the cyber domain and are growing together to provide the full range of effects a commander might employ in a contemporary multi domain operation.

About the Author


Lt Gen Richard CRIPWELL as a Brigadier served in Baghdad as the Director Energy Operations in Multi-National Forces – Iraq, as Commander Engineers in the Allied Rapid Reaction Corps, as the Assistant Chief of Staff for Intelligence at the Permanent Joint Headquarters in Northwood and in Kabul, where he was Director of the Strategic Transition and Assessment Group in HQ ISAF. Promoted to Major General, he was dual-hatted as the Commander British Forces in Cyprus and Administrator (Governor) of the Sovereign Base Areas. He then served as the British Defense Attaché in Washington and Head of the British Defense Staff in the United States. His most recent appointment was as Deputy Commander Operation "Resolute Support", Afghanistan.


Members of the 834th Cyber Operations Squadron analysing a cyber attack

175th Cyberspace Operations Group of the Maryland Air National Guard

National Perspective on Cyberspace Operations

Brigadier General **Giuseppe TORTORELLI**, Italian Army

We live in an era in which we cannot afford to keep the so-called "Fifth Domain" out of the military warfare equation: a vision immediately embraced by NATO in identifying cyberspace as the new Operational Domain. Fifth generation weapons have become the standard and digitization is considered a force multiplier asset for the Armed Forces of any Country, even if, on the other hand, it represents an inescapable vulnerability too. As we all know, many threats can impact cyberspace and can produce different effects directly on specific subjects through different vectors. Accordingly, the Armed Forces must be ready to counter these inherently and deeply asymmetric threats.

Some will opine that cyber weapons cannot stop a bullet for sure, at least not yet. However, they can strike and damage our precious information systems, logistic systems, and databases and delay or prevent the delivery of ammunition and spare parts on the battlefield. Our civilian and military reliance on GPS technology means that GPS spoofing, obtained by physical means such as a GPS jamming device or by soft attacks to the GPS satellites' constellations, presents a clear danger to naval, ground and air strike capabilities. Additionally, more and more complex and critical systems are now connected to the broader global internet. In fact, should we consider C2 systems, even on classified networks, immune from Distributed Denial of Service attacks? Indeed, the answer is obvious.

Cyber "activities" are an essential reality for State actors because the cyber domain is a powerful enabler and its effects a necessary and important contributor to multi-domain operations. Nevertheless, the cyber battle really depends on the capabilities (both on the technical and human skills' side) a Country can deploy "in the

Fifth domain

ITA Army - 33rd EW regiment in NAVWAR Exercise

field". In particular, the defense of critical infrastructure, both military or civilian, can only be achieved with high levels of planning and training pursued by any Country in peacetime, crisis, and conflict. We must be as prepared to counter and react to cyber threats with the same effort that we dedicate to physical and traditional military threats.

Speed of response toward a cyber-aggression is another crucial factor, especially in cases of complex, multiple attacks unless planned well ahead of time through a proper evaluation of the impact and ramifications of two aspects: cyber threats and activities.

In relation to the first aspect, attribution remains a thorny issue in the 5th domain. In fact, according to the Law of Armed Conflict and the International Humanitarian Law, without attribution a nation cannot react to an aggression from an unknown/uncertain source. Furthermore, even if, politically speaking, a Nation has the right to attribute a certain attack to a specific cyber Actor/State, a possible cyber response often includes more complex and challenging concerns than in the traditional military domain, like a traditional, targeted show of force.

In a NATO and EU context, cyber defense remains a common effort and goal. In this regard, several important initiatives such as the NATO Cyber Defense Pledge are important. The pledge is a firm commitment by the Allies, Italy included, to give the right (high) priority, at National level, to cyber defence aspects with the intention to increase resources and capabilities in the field within a structured National organization. It is quite more complex, to find common ground, within coalition frameworks, on cyber offensive operations which continue to be a national security matter. Nonetheless the importance of cyber operations, among the

NATO evolution on CYBER

Joint Command for Network Operations

various options available to a Joint Task Forces Commander, is so paramount that even NATO, whose posture is absolutely focused on Self-Defense, via Article 5 and, thus, on cyber defence, decided to rely on Allied Nations sovereign assets to be able conduct them. Accordingly, the *Sovereign Cyber Effects Provided Voluntarily by Allies* (SCEPVA) initiative, is a group of Nations willing to produce "cyber effects" when requested by a NATO Operational Commander.

In this "operational" context, in 2020 the Italian Armed Forces established the three-star level Joint Command for Network Operations (JCNO). This new command will ensure a robust cyber defense capability for the Italian Defense networks/assets, as well as the capability to plan and conduct cyber operations as a part of multi-domain operations. The leader of the JCNO will control three competences with Departments that focus on Network/C4 services, Cyber Defence and Security and Cyber Operations. Furthermore, acting as a Joint HQ, it also closely cooperates with the Single Services, Army, Air Force, Navy and Carabinieri. The command does so within an integrated cyber security perimeter and participates in a National Inter-Agency focused on cyber aspects, the *Nucleo per la Sicurezza Cibernetica* (NSC), chaired by the National Security Intelligence Department (DIS).

The JCNO is also cooperating with National Industry and Academia to develop several projects, including the development of a cyber range facility to provide scenarios for cyber exercises and an education and training virtual environment, open to the other Institutional Entities. Cooperation with other National stakeholders remains a cornerstone for a coordinated /comprehensive cyber defense posture of the whole Country. Moreover, the JCNO is proactively engaged with Industry and select Universities to develop not only defensive platforms and tools, but also effective capabilities to fulfill its mission to carry out full-spectrum cyber operations. This kind of osmotic relationship allows for the best of both civilian and military ideas to mix and allow for the creation of best practices.

In line with the NATO concept, which defines Cyberspace Operations comprised of CIS, Defensive and Offensive Cyber Operations, the JCNO has been structured on three pillars: the C4 Department, the Security and Cyber Defense Department and the Cyber Operations Department. This organization, established slightly more than a year ago, has demonstrated its effectiveness so far. Initial Operational Capability (IOC) has been achieved and we are now moving forward to reach Final Operational Capability (FOC). This quick creation and transition to active service is a daunting task pursued with steadfast determination by our women and men, our most precious asset and resource. In fact, most of the focus devoted to the constitution of the Command has been devoted to scouting, selecting and training military personnel of the Italian Armed Forces with established IT sys-

ITA JCNO

tems/cyber defence skills to achieve advanced competences in the cyber domain. Our personnel come from active duty military people, from all the Services, who underwent the aforementioned selection and, once assigned to the Command, started operating on the various systems/platforms while also attending advanced courses in accordance to different training paths defined in accordance to specific specializations.
This collection of intelligent, highlight skilled personnel is a huge investment, that must be protected and nurtured. Our structured organization must be able to provide an adequate level of technical and operational skills. No less important is, however, the capability to deliver this human "assets" where they are needed so the JCNO is structured to deploy its Cyber Operational Cells, highly specialized teams able to conduct full-spectrum cyber operations, in support of Theater Operations. This kind of units, specifically designed to support National contingents abroad in terms of Defensive Cyber Operations, are already operating in different Theaters where Italian Forces are deployed (Balkans, Central Asia, etc).

Conclusion

In sum, the 5th domain is a pressing reality that we cannot avoid or ignore. Recognizing its importance allows us to accept that operations in Cyberspace are more than enablers to support the traditional military domains. The 5th domain is an unavoidable aspect of contemporary peace, crisis and warfare. In future conflict, the domain will fully contribute to the so called "Effect Based Operations" which easily impact both the civilian and military spaces. A new approach and focus on full spectrum cyber operations is essential to inform a new way of thinking and preparing military forces for future conflict.

About the Author

Since 15 February 2021 Brigadier General Giuseppe TORTORELLI is the Chief of Cyber Operations Department of Italian Joint Command for network operations. From 2016 to 2020, he was the Commander of the Italian Army ISTAR Brigade (Tactical Information Brigade). From 2013 to 2015 he was appointed as Commander of 33rd Electronic Warfare Regiment in Treviso and afterwards he attended the Royal College of Defence Studies in United Kingdom. He has a master degree in Information Science at the University of Pisa and in Political Science at University of Trieste He served in the overseas operational tours as: Chief Communication Officer in 1999; Military Assistant of Multinational Division South East (MNSE) Deputy Commander in "Iraqi Freedom/Antica Babilonia" mission in 2005; Signal Battalion Commander in "Leonte" mission in Lebanon in 2008); and Italian Military Representative to the Hungarian General Staff from 2011 to 2013.

ITA JCNO

Cyber risk and new technologies

Massimo FRANCHI, CEO at F.M.S.

The increase in the level of risk caused by the pervasiveness of Information Communication Technology (ICT) in land operations requires new management skills, especially in the human resources employed in the field. Additionally, the associated technological innovations are modifying the organizational structures according to the logic used in the private sector or by the agreements with large multinational companies operating in the information technology sector. The data highlights that designing new architectures is not enough: we must return to a focus on the human operator and increase his or her awareness.

In our contemporary globalized world, the interconnected economy is now central to geopolitical choices. This complex scenario allows for a diverse range of national and international organizations to compete, from nation-states to multinational companies. Within a system in which vague threats and enemies have significant reach; the threats and their targets are no longer limited by geography. For example, hybrid and asymmetrical threats can be the most challenging to contain with traditional military forces. The fields of analysis and intelligence have become more fundamental, with current and future success being increasingly linked to artificial intelligence and machine learning. The importance of the "perimeter" - identified in broader terms also by the Italian Government with the establishment of the "National cybersecurity perimeter", as an extension of the transposition of the NIS directive - is now consolidated and widespread even if, within the world cloud and the related mobility is complex, even for the ordinary citizen, to clearly define the cyber ecosystem clearly and therefore its perimeter.
In the past, wars were predominantly won with national capabilities that have changed and evolved with technological advances. Examples include the number of soldiers, aircraft, and domestic industrial capabilities. Today creating and protecting intellectual property, as theft is now common by some nation states, is central to the future global balance of power. Maintaining information technology edge will now significantly influence economic, technological and military success. A failure to recognize the important of information technology will likely mean defeat in future conflicts.
Another fundamental element is "the time", related to cyber-attacks and defense. Interesting research by Nuix changes the traditional perspective from defenders to attackers. From this view they asked hackers how long it takes them to breach a network, which sectors are easiest to hack, and which defense mechanisms are the most challenging to overcome. Their research indicates that 54% of hackers say they can complete a breach, including perimeter penetration, by identifying critical and valuable data in as little as 15 hours. Essentially, in two working days!

The basic problem is that for 77% of hackers, the security team rarely or never notices what happened once the target has been compromised. Additionally, 9 out of 10 hackers say they can cover their tracks in less than 30 minutes after the breach. The motivations behind computer hacking activities in the civilian sector include financial gains, theft of intellectual property, and political activism, whereas in the military sector, the motivations are slightly different. Examples include the theft of confidential data and the interruption or damage to ongoing or future operations. Recent trends indicate how threats have become increasingly sophisticat-

ed by using specific tools, focusing on mobile devices, which are often less protected, and on large cloud computing with a few facilities with a large amount of stored data. Another area of interest for cybercriminals are social networks, where they can find a huge amount of personal data and that can be used to coerce individuals and possibly lead to penetrating organizations.

The typology of IT incidents can be divided, according to their degree, into events, incident, emergencies, disasters and crises. Going up in a hypothetical pyramid of potential damages, we can indicate that the trouble is rooted in a series of local *incidents* and requires management attention. In contrast, the *disaster* requires a larger impact. At the top and most critical point is the crisis, which is seen as a major event deriving from an incident that has gone out of control and with increasing severity for an organization. According to NIST[1] definitions, an *incident* is an imminent violation or threat to computer security policies, usage rules, and security standards. Instead, an *event* is any observable episode in a system or network. An *incident* can be voluntary or involuntary. A typical example of the first case is the targeted attack by a hacker, while in the second case, forgetting to activate the access list to a router.

Normally, the attacks carried out by nation-states or by third-party organizations operating for them in a covert mode are of the ATP[2] type. They are often characterized by a significant increase in resources, skills, and the use of sophisticated device's. In this case, the target is such because of who it is, what it does, or its IP value. The life cycle of the APT can be summarized as follows: a collection of information, initial exploitation, command and control, increase in privileges and data exfiltration.
A specific ATP threat can be composed of various complex attack vectors, including a mix of cyber, physical, and deception, and can remain unseen long after the attack. The target is scrupulously examined through careful planning that includes the anticipated study of countermeasures and the exploit of multiple vulnerabilities in a single assault through automated modules that target numerous platforms.

Stealth mode is accomplished by employing concealment and obfuscation techniques that involve hiding out of reach and view. In the event of an attack being blocked, attackers normally respond with further offensive actions by continually researching new ways to launch an

Example of potential damages from cyber events (graphic elaboration by Massimo Franchi).

attack. The typical target of an ATP attack, often seen as a springboard, can be the individual operating at all levels of the hierarchical organization. Targets at lower levels, such as less-senior leaders and contractors, are also of use to hackers since they may have less training and can still provide access to the broader system and thus access the higher echelons.

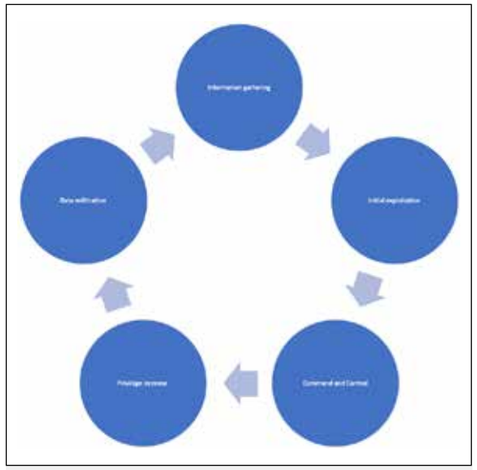
Today, no sector is immune from these type of attacks and their impacts can be catastrophic. Nightmare examples include manipulating industrial or nuclear plants' control systems, blocking critical infrastructure, and causing environmental disasters. In the military field, a typical impact can consist of the serious damage caused to the structures in the event of a conflict, with the loss of effectiveness of the device and the probability of success of the operations. In sum, all of the planning for a military operation can be near perfect and that operations can still easily fail at the hands of a well-timed and targeted cyber-attack.

To sum up, such a threat is enduring, adapts to the defenders' efforts, and maintains a level of interaction necessary to achieve one's goals. The APT is an expected part of current and future hybrid wars. As highlighted by NATO[3] and the US Army[4], conventional and unconventional means are used simultaneously or, according to the diversified and dynamic combinations of regular, irregular and terrorist forces are used represented on the field, criminal elements to obtain mutually beneficial effects.
In the terrestrial sector the concept of time is fundamental. In fact, with proper risk management, which includes the management of cyber risks, the goal is to attack the operational process of each environment, for example related to logistics, rather than the possession of data such as in the financial sector.

1 The United States National Institute of Standards and Technology.
2 Advanced Persistent Threats (APTs).
3 NATO Capstone Concept.
4 United States Army Doctrine Publication (ADP) 3-0.

From a military perspective, the US Navy[5] has improved the security of its supply chain by migrating its Oracle server-based ERP[6] to Amazon Web Services' GovCloud private cloud and by using SAP NS2. This choice is the first time that the Pentagon has employed, at least officially and to the satisfaction of former Defense Secretary Richard V. Spencer, such a system that will cut the time of use for six Commands and 64,000 global users. The US Navy, with this activity, which in the first phase took about three years and thousands of person-hours, is aligned with common business practices. This strategic choice includes aspects of compliance, audit, control, and unification in a single, more coherent system that reduces the attack surface and simplifies the infrastructure.

Amazon's Gov Cloud was born in 2006 and represents a global cloud infrastructure offered to government and public entities in which the customer chooses the developmental platform and programming language. The analysis of this new opportunity in which the data to be disseminated is stored in global department stores is now fundamental for the cyber military defense and the efficiency of the logistics support.


APT life cycle example - Advanced Persistent Threat, graphic by Massimo Franchi.

According to NIST, cloud computing is a model for enabling, via the network, widespread, easy and on-demand access to a shared and configurable set of computing resources that can be acquired and released quickly and with minimal management effort or interaction with the service provider. Undoubtedly, it allows organizations to save on traditional long-term costs in ICT by offering contemporary certainty. Today's commonly used platforms include *Software as a Service, Platform as a Service, and Infrastructure as a Service*.

Behind the cloud are the Service Oriented Architecture (SOA) architectures that support web services by ensuring interoperability between different systems and allow individual applications as components of the process. Many cloud providers are ISO27001, or FIPS 140-2 certified and are also subject to periodic audits. However, this does not make them immune and safe from attacks.

Of note, the European agency ENISA[7] summarizes the many advantages of the cloud that we must keep in mind. It allows you to set trends and lead the security market, with scalable, affordable, quick updates, and forensic testing and evidence. Alongside the advantages, ENISA also highlights weaknesses such as loss of governance, dependence on a provider, data isolation errors, lack of compliance, compromise of the management interface, difficulty in controlling procedures data management, incomplete cancellation of the same, and internal infiltration.

In this context, assuming that traditional structures are somehow constantly attacked or even compromised with known vulnerabilities in SCADA[8] systems in logistics systems and strategic and tactical communications, it is necessary to proceed through new strategic and operational paradigms. The connection and interdependence of networks and OT / ICS systems, with the significant commercial use of apps to replace traditional workstations, increase attack surfaces and requires dealing with risk management at a higher level.

According to Kyle Aldrich and other researchers, a "stealth" approach based on some essential elements is needed. These are the extended analysis of threat data, the ability to see, block and redirect traffic across all nodes on the network, the ability to download log data so that the log can be maintained and checked before it is accessed and modified by hackers. Additionally, the filtering of internet protocols is fundamental to the integration of threat intelligence feeds. Other experts contend that it is necessary to move from a vertical concept to full horizontal integration in all aspects of the operations and activities. The vertical idea is limited in the vision of cybersecurity as a world separate from the traditional military domains such as terrestrial, naval, air and space.

5 Modernization Takes Navy ERP to the Cloud, del 5/6/2019, US Navy.
6 Enterprise Resource Planning.
7 The European Union Agency for Cybersecurity.
8 Supervisory Control and Data Acquisition.

Cyber space operations specialists

An interesting questionnaire[9] distributed on a global scale in the ICT sector indicates that people are among the main elements that compromise the OT[10]. Specifically, 62.3%, for control systems, 21.8% for technology and processes at 14%. This figure confirms past observations, including the "Snowden case" that resulted in the sharing of secret documents on the PRISM and Tempora intelligence programs. Snowden justified his actions by saying that his purpose was: "to inform the public about what is being done in their name and what is being done against them.[11]"

Traditionally a defense system is composed of the Armed Forces and the companies that collaborate with them by developing projects considered strategic either independently or in collaboration with the Armed Forces and companies of allied countries. Within each organization, the sharing of information and the best practices implemented allows for more effective cyber security. The first step to be successful is represented by the human resources employed, also by making use of external agencies, universities or specialized associations. Their selection and training therefore is fundamental for an adequate defense.

In a turbulent and increasingly competitive geopolitical environment, emerging technologies such as artificial intelligence, the cloud, new 5G and 6G communications, and augmented reality require innovative computing, software, and advanced data processing that can connect every available sensor Additionally, they require new approaches in the field, such as the MDO[12] exercise, which include assets of intelligence, information, cyber, electronics, warfare and space units not only in support of operational units.

An approach based on detailed and thorough risk management, which incorporates assessing all forms of risks and the likelihood of their occurrence, including operational and financial impacts, is also very useful in the military field. The individual Armed Forces, often operating in foreign theaters, face a diversity of hybrid threats, internal and external. Considering the stakes, it is essential to extend the concept of cyber security not only to the world of Italian and NATO defense, but also to the tens of thousands of companies operating in the sector that represent the "first line of defense" against blatant hostility from some nation states.

Conclusion

In this perspective, the fifth domain is not just a conceptual environment, but something of concrete related to hardware, to the raw materials necessary for manufacturing and the supply chain. Risk management should also include these areas, which are now led mainly by multinationals and not by states (except China). In fact, behind every new technology, we find a technological infrastructure whose possession, protection and maintenance become strategic. In addition to looking at international threats, we should focus on internal vulnerabilities, in the awareness that cybersecurity is now part of a state's strategy. The first vulnerability is the human being for whom it would be important to increase cyber skills at a technical and managerial level in all organizations, obviously starting from those considered critical. Cybersecurity should become part of the education of citizens who, in a borderless world, may find themselves easy prey to a bigger game than nation states or unscrupulous criminal organizations are playing them.

About the Author

Former Italian Army officer and CEO at F.M.S. consulting, Massimo FRANCHI is Research Fellow, member of DiMeTech-Lab at the University of Parma and Adjunct Professor at II Level Master in Intelligence at the University of Calabria. He contributes to "Rivista Marittima" monthly magazine of the Italian Navy.

9 SANS 2019 State of OT/ICS Cybersecurity Survey.
10 Operational Technology.
11 https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.
12 Multi-Domain Operations.

Security and Space systems

Massimo CRISCI, Head of RF Systems Division (ESA)

On the one hand, space systems are increasingly central to the daily lives of European citizens and the services provided, address the needs of a wide range of users and are essential to the global economy. Much of the world's strategic infrastructure, such as communications, air transport, maritime trade, financial and other business services, weather and environmental monitoring and defence, depends on space systems assets, including satellites, ground stations, data links, etc. Alternatively, the access and development of space infrastructure is becoming possible for an increasingly larger number of new players. With access comes the possibility to change business models, the number of potential applications, and the development cycles of these new missions. As a consequence, space infrastructure is becoming more critical and subject to not only to safety threats but security threats alike. It is currently critical to protect these assets from intentional or unintentional harm or damage. This is valid not only for the more traditional military applications but more also for the civilian ones. But providing security to such a diversified sector comes with its own challenges and a combination of bespoke dedicated solutions. Additionally, security will require a wider adoption of good common security standards and practices including new technological elements, last but not least cyber security aspects. Cyberattacks are in fact considered the fastest growing crime and are increasing in size, sophistication, and cost. To be protected from damages, both private and public enterprises must increase their information technology security spending. This discussion will address challenges and potential solutions.

The criticality of space systems

Space is a diversified and variegated context. According to the UCS Database, as of January 2021 there were 3372 satellites orbiting around the Earth, with the vast majority of the countries possessing at least one satellite in space. Space has evolved from the defence playground of a few advanced space agencies, to a domain in which every country can possess and manage a satellite.
Satellites are placed in different orbits: Low Earth Orbits includes a few hundreds of kilometres to Highly Elliptical Orbits up to and beyond 40,000 kilometres. The systems that orbit the earth intertwined into our daily lives. Examples include critical communication infrastructure, weather forecasting, disaster recovery, intelligence, and science and exploration. European examples of those systems range from the Global Navigation Satellite Systems (GNSS) that provide accurate timing and navigation capability to users with GNSS receivers in all possible application domains of road, maritime, air and pedestrian users. The Copernicus Earth Observation system and the Sentinel satellites, offer global earth observation capability and provide timely information supporting land and marine management, emergency response and civilian security, understanding and mitigating climate change, improve the knowledge of the atmosphere. The meteorological METOP and MTG satellites monitor weather patterns, the movement of storms and other cloud patterns, observe other phenomena such as city lights, fires, pollution, snow cover, ice mapping, boundaries of ocean currents and flows. On the commercial side, Satcom operators provide services to broadcasters, Internet Service Providers (ISPs), private and business users, governmental, military, and other sectors, reaching the cities and the most remote polar locations, while a fast growing private and institutional demand for optical and RF earth imagery is creating fast growth in the EO Data market. Space systems

A virtual reality simulator at Johnson Space Center

are becoming de facto foundations of national or supranational critical infrastructure and the services that need every single day.
The increased reliance of other sectors on space assets and services for their own success and competitiveness puts pressure on the need to address security threats which endanger critical assets in space and their supporting infrastructure on Earth. While space engineering has a long tradition focusing on safety and reliability, given the harshness of the launch and space environment, security introduces the dimension of intentional, man-made threats in addition to the traditional threat sources coming from the natural environment, technical failures and unintentional human error.

New Space

But the space context is still quickly evolving. In the recent past, there was a transition from an institutional to increasingly commercial sector; from the domain of space agencies and few specialized satellite operators to our contemporary time where every company could build a satellite, wider access to Space being key in this transition. Some people this change is a revolution, called “new space”.
While it is difficult to define “New Space”, it may be easier to identify some of the new trends. Firstly, it is characterized by the emergence of new companies, some large players not traditionally associated to the space business, some others who are completely new start-ups with novel business propositions. Those are primarily business oriented, pushing for lowering the costs and the shortening the time to market of their products and services. Examples include, the 900 out of the 3,372 satellites orbiting belong to the Starlink constellation, a SpaceX project that aims to launch up to 12,000 mini-satellites to provide worldwide internet services. The first launch was only in 2018 and their services are already on sale in 2021.
The commercial transition is now impacting all the application fields while originally, the largest interest was focused on Satcom. Companies are offering images of the earth, monitoring and tracking of ground assets, worldwide connections to for devices and even planning the commercial exploitation of humans in Space, and they are competing with big space agencies for planetary exploration. Concurrently, this change is driving the application towards more and more challenging scenarios, from the open air, within the sky context, to the urban and indoor environment, involving more demanding features, e.g. safety aspects for the vital communication, integrity for the GNSS corrections to trains and planes, support to low power devices and coverage for massive number of users with connected devices.
The transition also has implications for the architecture of the Space systems towards more capable architecture, more powerful instrument and payload on top of massive constellations. Large constellation, sometimes mega-constellations, of small relatively cheap satellites compared to traditional single, powerful ones, optimized production chain, design to produce. Additional changes include short system lifetimes, a reduced need for expensive qualifications, less powerful individual instruments and payloads, big data aggregation on ground for products generation, reconfigurable and reprogrammable architectures, based on SDRs solutions for ease of platform reuse. The major reutilisation of ground technologies and components also in Space, massive digitalization, usage of COTS and standardized components, operations offered as a service by new operators, ground segments largely intertwined or integrated with terrestrial applications.
While at the user equipment level this integration is pushed in most applications e.g. phones, and wearables, integrating in a single chipset 3G/4G cellular communications and GNSS, terrestrial service providers are rather new entrants in the space sector, where Amazon, Samsung, and other large corporations, are showing concrete interest in deploying their own constellation.

Security of Space Systems

Now we must examine the security of critical space infrastructure
Problematically, not all active missions are adopting to a security informed frame. The variety of the use and purpose of Space mission, military, governmental, institutional, commercial, scientific, educational, etc., have led in the past to different choices, depending on the criticality of the services and assets, explicit requirements for asset protection, perceived risks, vulnerability and attack opportunities.
But the situation is changing. Whether this is due to commercial pressure to protect lucrative assets, or the need of public institutions to protect their expensive systems and the reputation associated to their loss, or maybe just an increased awareness of the risks, the perception of the space stakeholders towards security risks is growing. Moreover, the proliferation of space objects in a potentially crowded orbit areas, implies the assumption of a certain level of collective responsibility toward, and requires the adoption of a minimum level of assurance to operate. If this is not happening regulations may be enforced. From a time when civilian space missions were flown without much concern about security, we have moved to a time with a pressing need for protection of these missions.
Space system are interconnected with Cyber Physical Systems (CPS) with potentially large Ground and Space networks, worldwide distributed, composed of a mixture of bespoke and COTS HW and SW components. Space assets are typically long lasting, difficult to maintain once deployed, reachable only through powerful ground stations and feeder links, and are supplied by well-known and highly specialised companies. From this point of view, they were always considered quite secure by construction, the ultimate protection achieved through strong link encryption acting as a firewall to the spacecraft internal payload and avionics subsystems.
Is there anything special in space that requires a dedicated approach for security? The answer is Yes and No.
Yes, because systems have to deal with the specific restrictions and constraints of space missions including maintainability, long lifetimes, limited on board computational resources, autonomy of a large part of the spacecraft operations, meaning that we cannot unplug the “space” device from the network when we want. Any ground derived Hardware/Software solution to be brought in space must be specifically qualified for space survival. The higher the security level, the more security is required for the specificity of the CPS as getting closer to its HW and SW constituents, e.g., generic anti jamming, and anti-spoofing needs to be tailored to specific space link. This requirement makes it difficult to derive complete solutions from other sectors and assume they will protect space assets as well.
No, because the same protections required at the base station or control segment of a large cellular network, should be in place in the control centre of the satellites, following the same techniques e.g. cryptography, process and even procuring the same COTS equipment. In this respect a lot of technologies can and are already a spin-in of more known terrestrial applications for cyber security.

The nature of the threats

The ultimate security objective of a space programme is to safeguard the integrity, availability and sometimes confidentiality of its data, assets, or services. The nature of the threats is varied and can impact various space components: examples are attacks on satellites, by targeting their control or mission segments, perhaps taking over a satellite to exploit its payload, shut it down, alter its trajectory (transforming it into a “weapon”), or destroy its solar cells through exposure to damaging levels of radiation. Attacks can also target the ground control centres, the associated networks, and data repositories, leading to potential global impacts. The link may be intentionally compromised via jamming and spoofing, causing intentional disruptions or deceptions that impact the uplink or downlink of signals to disturb the operations and/or delivery of services.
It is true that attacks in space are seldom in the spotlight. Still, publicly available information points to the fact that security breaches have affected navigation, positioning, and timing systems. Examples are jamming, spoofing, corrupted data, etc., including the space, ground and user segments), earth observation satellites (including takeover, ASAT demonstrations, blurring, etc.), and satellite communication assets (jamming, interception of data, etc.). On Sep-

tember 7, 2018, the French Defence Minister publicly declared that a French governmental satellite, Athena Fidus, had been spied on by Luch-Olymp, a Russian governmental satellite. The Minister further suggested that this eavesdropping spy satellite was then observed as it manoeuvred to monitor other allied space assets. This was not the time this occurred since Luch-Olymp had already been caught in the proximity of U.S. Intelsat assets in 2014 and 2015 for espionage purposes. This is the reality of space today.

Related to users, numerous examples of satellite jamming have occurred in recent years both in the civilian and military context. GPS signals were regularly jammed during the Crimean crisis in 2014. Spoofing is a type of signal-based attack that aims to deceive a receiver by broadcasting incorrect signals that resemble genuine signals, or by re-broadcasting genuine signals captured at a different location or time. One of the most notable examples of spoofing took place in the Black Sea when the U.S. Maritime Administration reported 20 affected ships near the coast of Novorossiysk. Another example is the disruption by North Korea of PNT signals used by South Korean aircrafts and ships. The most acute attacks occurred in March 2016 when more than 1,000 aircraft and 700 ships were affected.

To create awareness about those threats, the U.S. Department of the Air Force and Department of Defense (DoD) recently sponsored the Space Security Challenge 2020. The hack-a-thon style event aimed to spark interest in space defence systems and to join cyber security professionals with satellite designers. Hack-A-Sat (HAS) 2020 was a satellite hacking contest run by the US Air Force and the Defense Digital Service. The HAS qualifying round counted 2,213 teams registered and over 6,000 players competing in the Jeopardy-style Capture the Flag (CTF) competition. The final event, which included mock satellites "orbiting" on a custom-built carousel, was held between August 7th and 8th and featured 8 teams with players from 12 countries competing for a chance to win part of the $100,000 prize pool.

Cyber Threats and Cyber security

The cyber domain requires a special mention. Space system security must be regarded from a holistic point of view. The attacker will in fact search for the weakest point, and this maybe any cyber component of the Space system infrastructure. Security shall in fact address not only space segment, ground and user segment and their operations, but all the cyber elements those segments contains, their SW, Operating System, their supply chains etc. Satellites and the other associated space and ground assets of any space system, just like other parts of the digitized critical infrastructure, are vulnerable to cyberattack.

Vulnerabilities can arise throughout the system lifecycle, including development and production. Indeed, loopholes in some satellite hardware, both electronic components or software can be intentionally added and/or exploited by offenders who conduct cyberattacks. This technique is referred to as "backdoors" and can directly impact the safety of space systems. The cyber-threats are fairly wide ranging: hardware and software can be maliciously modified undetected and the malicious capabilities could be triggered later. Within the context of a space mission's supply chain, some on-board components available on the market may contain spyware or logic bombs. Another source of risks in the supply chain is the external personnel who are involved in the outsourced services, or even social engineering risks, including from within one's own agency. The globalisation of manufacturing capabilities and the increased reliance upon commodity software and hardware for ground segments has expanded the opportunities for malicious modification in a manner that could compromise critical functionality.

Example of cyberattacks have included hacking attacks on communication networks, targeting control systems or mission packages, the ground station SW, the VSAT terminal etc. In 2018 IO Active revealed major satellite Communication and operating system vulnerabilities at Black Hat USA 2018 & DEF CON 26, and demonstrating how some Satcom equipment were vulnerable to potential attack. This realization caused manufacturers to take prompt corrective actions.

Cyberattacks vary from the simple to most sophisticated attacks. Some can aim for System Compromise, to obtain temporary control of a system and gain the capacity to execute arbitrary commands or to gain a foothold in the network to carry out other attacks. Another goal is service disruption, to prevent a system from performing as expected with consequences ranging from reduced quality of service to total system failure. data exfiltration steals sensitive information from a target for reconnaissance, strategic intelligence, theft, or to expose secret information. Bad data injections use undetected incorrect data (e.g. erroneous TT&C data) within a system with a range of possible consequences. Finally, advanced Persistent Threat (APT), seeks extended access to a system for permanent and undetected capacity to access system information or take control of the system.

Cyber-attacks can target individuals, companies, and public institutions, but also democracies. Some attackers could seek to destabilise a country by undermining public trust in government institutions by challenging core values of modern society with disruptions to economic or public services and institutions. Hence, building strong and resilient cyber security has thus become a worldwide priority. The International Telecommunication Union (ITU) defines Information Security/ Cyber Security as follows: "The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, the organization and the user's assets". These cyber threats are now at the core of a multidimensional phenomenon: hybrid threats, which combine "coercive and subversive measures using both conventional and unconventional tools and tactics." An increasingly hostile and aggressive cyber environment in a time where connectivity is ubiquitous raises the importance of cybersecurity. Hence, building strong and resilient cyber security has thus become a priority and a critical requirement for next generation space systems.

The chief of space operations for the U.S. Space Force

Challenges of Space system security

The biggest challenge for Space system security in the next years will be to ensure that the growth we observe in terms of players and economy of Space is followed by an equivalent growth in the adoption of the correct security frame for their missions.

For the most demanding institutional missions, the challenge will be to remain up to date with the evolution of the threats.

For the more commercial ones where the costs and time to market are as driving as much as the service performance, the challenge will be to make it efficient and affordable. This requires the adoption of standard architectures and processes, the adoption of common practices for the protection of the ground and space assets, the availability and interoperability of the various building blocks in time and at the right costs, sharing of threats and vulnerability analysis.

What is the technology needed to counteract the specific cyber threat faced by our space systems? Is the so called "new space" paradigm changing the picture for what concerns cyber security needs and solutions? Are new requirements emerging?

Technology to support Space system security

It is impossible to address in a short paper all the technologies that are and can further contribute to the security of a space system. As said before, security should address the problem from a holistic perspective, including ground, space, user components, the links, the data at rest and in transit, supply chain etc. A dew recommendation may be of value.

Security architectures and key building blocks

The first element to consider is the architecture itself. Guaranteeing security may require com-

A training scenario at the Asymmetric Warfare Training Center on Fort A.P. Hill

plex expensive and long-term design and assessment processes. Therefore, security needs to rely on standard architectures and building blocks, whose effectiveness has been proven and tested in operation by many users.

For ground infrastructure we have to keep up with terrestrial trends with the usage of standardized technology spinning in best practice and techniques from the most traditional ground segments and resilient networks, like the monitoring of the traffic, the detection of anomalous behavior of SW components, support for forensic and data analysis etc. A large potential for spin in from mainstream computer network defence technologies into ground system networks exists for intrusion detection and prevention systems. Existing modular implementations should be extended by space-specific protocol add-ons as opposed to trying to develop a complete, dedicated tool set. For the on board space networks, such as data handling inside satellites, existing intrusion detection and prevention concepts can be translated to the significantly different space data networking architectures and protocols, security monitoring capabilities including incorporation of threat intelligence information suitable for space missions, definition, implementation and evaluation of active defence (e.g. deception) techniques for reliable early warning on attacks, development and implementation of Machine Learning based techniques for enhancing threat hunting capabilities etc. In a potentially contested RF environment also RF awareness, localization of the radio threats capabilities, protection of the links etc.

Space is moving from simple topologies, like one or more satellites without interconnections, with limited scalability, for which just a smart end-to-end security solution at space link layer has always been considered sufficient, to complex topologies, such as large constellations with inter-satellite links and millions of users that require scalable space network security architecture, necessarily shifting from custom-specific developments (system, sub-system, components), bespoke SW and HW and ad-hoc security design to COTS-based solution, MOTS, reuse/spin-in from terrestrial technologies and standard secure on-board architecture.

On the spacecraft side, solutions need to address the low maintainability and the long lifetime of the missions through strong secure re-configurability and re-programmability after launch. Processing architecture relying on secure partitioning and enclaves or Trusted Processing Module, allowing secure booting, identification and remote attestation of nodes, including HW authentication concepts will be key. Architecture resilient to temporary denial of links, secure autonomy of the spacecraft, and autonomy of the operations need to be addressed as well.

The Space links

For what concerns the links, most of the space systems protect communications between ground control and spacecraft only with a firewall approach. This assumes implicitly that spacecraft processor(s), microelectronics and SW integrity are not exposed or that the supply chain can be trusted. We need to be prepared to move to defense-in-depth security architecture with several security controls/functions (communications and node processing security) and force supply chain security. Strong dependability and recovery capabilities are necessary.

Security is also linked to the Communication protocols. Contemporary standards are based on CCSDS Packet-based operations, or a combination of CCSDS/IP Packet and File-based operations, whose security features are covered by CCSDS Space Link Services with Security, intended to replace proprietary data link layer security solutions that were implemented in absence of a standard. It is important to develop and validate SDLS prototypes as a short-term priority to ensure security interoperability and to speed up the development of flight hardware to improve availability of affordable implementation for generic mission types. Standardised security solutions for other layers of the CCSDS space networking communication stack (e.g. packet/network layer, application layer, DTN, etc.) are still in early R&D at this moment. It is envisaged that with communication management moving up the stack towards a networked environment also in space missions like for example larger constellations, these layers need to be protected and security standards matching the needs for space networks needs to be developed and validated in the medium term. Spin-in from terrestrial techniques is expected, but limited by low-bandwidth, high delay communication channels in space plus low computational power and high reliability requirements for spacecraft avionics.

On the Physical Layer Security, resistance to jamming and interception can be addressed with cryptographic spread spectrum technology. Complementary communication techniques like advanced forward error correction and robust frame synchronization are also part of this research and development effort. For the most secure mission, anti-jamming and active cancellation of interference may become a needed capability.

The Cryptographic elements

Generally contemporary Key Management solutions for space missions do not go beyond a simple negotiation mechanism for point-to-point links. Those are not adequate to support more complex security architectures. Key management is one of the best understood security problems in terrestrial networks, so once space missions consist of many nodes, terrestrial concepts can be spun in, under the four constraints already mentioned above. Another important dimension is the logistics of the key loading and the protection of the Satellite secret(s) once loaded before launch. Specific measures to securely inject sensitive material into spacecraft before flight and to protect spacecraft access once loaded are necessary. Ideally we should move towards secrets upload during launch or post-launch phase (LEOP) of the material to reduce complex logistics on ground.

Cryptographic algorithms used in space missions today directly evolved from terrestrial solutions, that can be decades old, Symmetric (AES in various modes in an example both for traffic and key management (256-bit key). Moving towards asymmetric schemes, next generation quantum computer-resistant asymmetric cryptographic algorithms for key exchange is foreseeable and need to be analysed and validated to confirm their use. As in other areas of cyber defence mechanisms, agility/flexibility during implementation will become a much more important aspect given the rapidly evolving threat environment. From inflexible (no change of cryptography once specified, developed, tested and flown, to potentially flexible architecture with Secure In-flight upgrade.

Regarding Quantum Key Distribution (QKD) technology, it will most likely play a role in practical secure implementation. Potential applications could be envisaged for individual, highly sensitive links with low message volume, tolerance to high latencies and very high protection needs, once fundamental research on implementation security aspects such as novel side channel attacks have sufficiently progressed.

Other elements

Related to software security, today's commercial software is being developed following rigorous secure software engineering practices. Large catalogues and databases exists for identified requirements, vulnerabilities, risks, attack trees, best practices, etc. In the space domain, software security is becoming important in particular also for unclassified missions. Standards, methodologies and tools are being developed including elements to support SW security assurance processes, for highly classified mission still relying on National Security Authority regulations but for unclassified missions to follow emerging ECSS Security Engineering Standard(s).

Finally, protection must be extended to the user segment. Architecture of the space systems may be quite different. From a centralised repository of the space products, e.g. for scientific and earth observation mission, to millions or even billions of distributed users and equipment, in Satcom and GNSS applications. The security problems spanning from protecting large data infrastructure, to the one of securing information on a handheld device, typically the weakest point, normally directly accessible to the hacker for vulnerabilities analysis, is constrained by the cost and faster turnover of technology.

Conclusion

The role of Space has changed and continues to change as the technology becomes interweaved into our daily life and applications, this making it part of our critical infrastructure. The economy of space has also changed with the introduction of new players and new commercial drivers who are guiding the design of their systems, including profitability and time to market. Since space technologies are used for the delivery of various services, any type of attack can thus affect the users of those services including unmanned aerial platforms or cruising ships and their communications. This creates more appetite for attacks, an increase in the threat space and vulnerabilities, and the need to protect infrastructure, and user segments against them.
Protecting space infrastructure requires a collective and urgent effort in terms of resources, process and system capabilities. A concerted effort for the adoption of a standard architecture, the development of the associated building blocks, the creation and utilisation of standards and good practices are essential. We need to make sure this is happening on a wider scale to avoid exposing not only the economy, but also the precious resource space has become for everybody, to the risks of assets and data compromise. To support the adoption, the role of the public and government institution will be fundamental as well, through the development of Standards and the regulatory frames.
The shift from the use of mature terrestrial solutions tailored to the constraints of space will be important to avoid the need to re-invent them, and to focus the development of bespoke SW and HW. The latter is where research is still required and is also the focus the majority of its efforts.

About the Author

Massimo CRISCI is currently the Head of RF Systems Division in the Technical Directorate of the European Space Agency (ESA), where he has been working since 2004. Prior he was the Head of the Radio Navigation System and techniques section in which he has also worked as engineer in support of ESA Navigation programs, like GALILEO and EGNOS. He is responsible for the technical and strategic management of activities in the RF System division, in which 70+ staff and contractors provide expert support to all ESA programs in the RF system and technology domains, which include Navigation, Telecommunication, Earth Observation, Science, Human and Robotic Exploration, and Security. Massimo Crisci has a PhD in Automatics obtained from the University of Bologna (IT) and a master degree in Electronics Engineering from the University of Ferrara (IT).

Astronaut Edward H. White II, pilot of the Gemini-Titan 4 flight

Can AI help military organizations in their cyber security decision–making process?

Emanuele GALTIERI, CEO of CY4GATE S.p.A

The Big Five Tech Giants (Alphabet, Amazon, Facebook, Apple, and Microsoft) are known as innovators. They, along with thousands of start-ups, are striving to leverage Artificial Intelligence (AI) technologies to inform decision making to adapt to dynamics and increases in complexity. There is a common belief that all decision-making strategies should be improved in terms of speed, accuracy, personalization, scalability and adaptability. This need can also be extended to critical infrastructure Security Operations Centers (SOC), that enhance intrusion detection and incident response capabilities in cyber security networks.

Network monitoring generates data at high speed, and this process often leads to the collection of a large amount of different noises. Analysts might be so busy executing tedious and repetitive data triage tasks, that they could struggle to focus on in-depth analysis for further decision-making action plans. That is the reason why it is critical for military organizations to implement new technologies in cyber situational awareness.
Before analyzing how technologies can be used to enhance the decision-making process, we should consider the OODA Loop paradigm, developed by strategist and U.S. Air Force Colonel John Boyd. OODA stands for Observe, Orient, Decide, and Act as part of a cycle or loop of decision making.
Reaction times, effective decision-making strategies, and quick actions are crucial in aerial combat. The enemy always gets the upper hand in case of slow reaction times: if you do not make changes over the course of time, the probability of failure increases. This is also true when deal-

A network in the digital era

ing with cyber resilience and cyber deterrence.
Governments, corporations and other organizations are currently using the OODA loop strategy, as it clearly represents the processes we naturally follow when learning, growing, and thriving in dynamic environments.
Before describing the main features of the OODA loop, we will focus on the Loop concept itself: the continuous feedback provided by the OODA strategy provides institutions with additional information after each use or cycle.
The first step is to Observe, so as to achieve situational awareness, to understand an environment, and of identify evolving trends. After collecting as much data as possible, we move to the Orient phase, in which an organization uses inherent and learned capabilities to analyze, assess and synthesize data. The primary output goal is obtaining efficient options to inform a decision making process.
Next, the Decide phase, that aims to recommend the best choice among the options generated during the previous phase. Finally, Action involves the actual execution of the selected decision and thus, the loop is closed. After which the loop can become a recurring part of planning and execution processes, with adjusted speeds that can be adjusted as required.
Returning to the topic of AI, systems that are augmented with AI can be used to either assist human decision makers, or to replace them. When using the OODA Loop model, we can more deeply explore AI and decision-making strategies. The three main methods in which AI can be inserted into an OODA Loop construct are as follows:

- Decision Automation: The Observe, Orient and Decide stages are fully automated, while the Act phase is often semi-automated;
- Decision Augmentation: The Observe and Orient stages are automated, after which the AI partially supports the Decide phase, providing users with some options to lead them to the final evaluation and to finally perform the Act step later;
- Decision Support: this Intelligence technology carries out the Observe stage to provide the human users with proper insight, and takes them onto the Orient phase. The human user is in charge of the Decide and Act later stages.

The application and use of the three methods, depends on specific scenarios. Generally speaking, the Decision Automation method is most applicable if the user needs to apply a rapid decision-making strategy, or when the scenario appears to be easily solvable.
Alternatively, when one deals with a more complex situations and when the user has time to deliberately think how to best react, one can choose for the Decision Augmentation method.
Finally, during chaotic scenarios, implementing the Decision Support method is the preferred solution.
The use of AI in a military environment still creates uncertainty for those involved. The main concern is the impact of the transferring decision-making processes for military operations to non-human intelligence. The life and death circumstances associated with military operations and the importance of following national and international rules and conventions regarding the use of military force are examples of the plethora of concerns.
Accordingly, many organizations emphasize the role of AI as a tool that augments or supports to

Cyberspace Operations Group

A cyber-warfare specialist

human decision-makers, rather than replacing them. As the core concept of automation, this is also a much more familiar and seemingly safe concept.
This vision can be shared, even if a Continuous Intelligence will be available for our use in the near future.
Furthermore, in our view, one can implement a Continuous Intelligence to enhance the Command and Control networks of the Armed Forces, in which an of myriad sensory input and data come together – and are revealed as waterfall or simultaneous orchestrated responses, and AI is the Conducting brain.
Recently, a Decision Intelligence platform has been implemented, based on proprietary algorithms, with the aim of enhancing descriptive, predictive, and prescriptive analytics. Descriptive analytics answers the questions: What happened? – What is happening? and it examines the data or contents retrieved in the past in order to understand what is actually going on in an organization. Through this analysis, organizations may learn from their past behaviors, and foresee how the latter could influence future outcomes. Predictive analytics: What will happen? ingests data silos and feeds into an AI Machine Learning / Deep Learning models to try to predict future outcomes. It is crucial to underline that we are referring to estimates of probable future outcomes. Prescriptive analytics answers the question: How can we make it happen? and it provides the user with advice and recommendations that are informed by AI algorithms that execute a What if and an Optimization Analysis. The platform suggests possible outcomes before implementing a decision-making strategy.

Conclusion

The platform's goal is to show data and solutions in a clear, easy to understand way, so users can understand and evaluate complex analysis processes, to make decisions faster. A wide range of technologies, including Dashboarding to Continuous intelligence and Artificial intelligence, can make the decision-making process easier for military organizations. Additionally, they can strengthen Critical Infrastructures' prevention, detection and reaction times in case of Cyber-attack attempts. Therefore, the challenges before us is balancing in the best possible way the selection of the optimal combination of these technologies to be able the achieve the desired results.

About the Author

Mr. Emanuele GALTIERI is the CEO of CY4GATE S.p.A (Elettronica Group), a Cyber Intelligence and Cybersecurity company, listed on the Milano Stock Exchange. He was DEPUTY CEO & General Manager of CY4GATE. He joined ELETTRONICA in 2008 where he held several important roles. He was previously a Carabinieri Corps Officer. He has a degree in Law at the University of Rome, the Degree in Political Sciences at the University of Trieste and a MBA at the Luiss Business School in Rome. He fluently speaks Portuguese and English.

NATO, European Union, and National perspective on Cyberspace Operations

Lieutenant Colonel **Gianfranco ELENA**, Italian Army

Consider this possible scenario: a NATO country is hit by a cyberattack that takes down much of the national critical infrastructure for several days. The attack causes malfunctions in the electricity and gas networks. ATMs are not dispensing cash and backup power for hospitals is close to running out. Hundreds of thousands of people are suffering due to the negative impacts of the attack and the populace is looking for answers and a solution.

The first question that Allies policy makers might debate is whether NATO should respond to such an attack with a military response. But several problems immediately arise. For example, who would coordinate cyberspace intelligence activities and cooperation with national critical infrastructures? How would NATO know how to accurately attribute the attack to a nation or a transnational organization? Should NATO use a cyber counter-attack that inflicts equal damage on the attacking nation or respond with conventional military forces?

The complex issues associated with this possible scenario were discussed during NATO Rapid Reaction Corps Italy (NRDC-ITA)s recent first edition of an international Cyber seminar on the "Future of Cyberspace Operations and Security of National Critical Infrastructures" on March 3, 2021. The event aimed to increase the general knowledge of NATO, European Union (EU) and national cyber strategies while encouraging a deep discussion, with academics and military experts. Specifically, the what emerging technologies should be strengthened and developed to improve NATO cyberspace capabilities. Of note, Lieutenant General Cripwell - Deputy Commander of NATO Land Forces – presented the NATO perspective on the future of Cyberspace Operations (CO); Mr. Martin Konertz - General Director at the European Defence Agency (EDA) - discussed EDA support to shape the EU Defense initiatives on cyberspace operations; Brigadier General Tortorelli - Chief Cyberspace Division at the Italian Army - addressed the Italian outlook on CO; Prof. Roberto Baldoni – Deputy Director of the Department of Information and Security - presented the national plan for security of critical infrastructures; prof. Stefano Zanero - University Politecnico of Milan – illustrated the most important challenges related to the implementation of advanced Cyber situational Awareness (CSA) and intelligence systems; dr. Massimo Crisci - head of space systems division at European Space Agency (ESA) - discussed the main threats and vulnerabilities of space systems; and Mr. Eugenio Santagata - CEO at Cy4Gate- described possible solutions to improve prevention, detection and reaction to cyber-attacks.

Based on the fruitful event, there are a few points that it is worth to recap in order to identify some takeaways from this seminar and pave the way ahead for the next one.

First of all, the speakers confirmed that the Cyberspace domain will have a key role in the future conflicts. Cyberspace threats are increasing in frequently and their impacts are becoming more impactful. Accordingly, a single NATO country may suffer unprecedented consequences even without triggering conventional NATO Article V Collective Defence Response. Moreover, it could be difficult to associate, with any certainty, an attack to one specific country or organization since some governments may rely on private cyber contractors to conduct their malign activities. In particular, if the attribution of the attack is not possible or the role and responsibility of the adversarial government is not clear, it could be hard to take the decision to retaliate. For example, in the case of a major cyber-attack against a nation's power grid, NATO could be under immediate and tremendous pressure to respond. But if the Alliance retaliates and the cyber forensic analyses are wrong, then the reprisal will have unreasonably and could accidentally start a war. Then, what are the possible solutions? One option could be to launch a counter-attack that causes similar cyber damage on the adversary. Alternatively, if the targeted NATO country had recovered from the attack with minimal real damage, then this cyber counter-attack might be seen as disproportionate. Moreover, even if the consequences of a cyberattack were serious and NATO countries knew the identity of the guilty party, it would be better to carefully consider the use of cyber-attacks because they can have unanticipated consequences. It is still difficult to assess and avoid collateral damage when using cyber offensive tools and the possibility of unexpected effects is significantly greater. Cyberspace operations increase the level of uncertainty to warfare and make it challenging to both to deter and respond. It will take additional time and reflection to approve a faster and effective decision making process as well as a great deal more research and analysis, before the problem can be fully understood.

Secondly, NATO is clearly an appealing target because successful cyber-attacks against the Alliance may have significant international ramifications and media coverage. In fact, in the last years, enemy cyber actors have escalated their objectives from disruption and espionage into information operations targeting the Alliance cohesion, decision-making, and effectiveness, with the aim to make NATO ineffective. The leading role of NATO as an organization capable to ensure stability could be at risk if NATO does not consider potential critical shortfalls, such as: partial synchronization of cyberspace effects across all domains, limited cyber offensive capabilities, and a lack of trained personnel. Additionally, steps could be taken to recognize the cyberspace as an operational domain and establish the SHAPE Cyberspace Operations Centre (CyOC) to plan, synchronize and direct Cyberspace Operations (CO). Due to the extremely fast tempo of cyberspace operations there is a strong need to speed up all the processes to accelerate the pace of the current strategic and technological changes. Operations in cyberspace need to become a fully integrated part of NATO capability to deter hostile activities and to protect NATO's freedom of maneuver in all operations.

Another interesting point of discussion was related to the challenges of understanding and adapting to new vulnerabilities originating from the adoption of emerging technologies such as: Artificial Intelligence (AI), Machine-to-Machine Interactions, 5/6G systems, and the Internet of Things (IoT). Defenders cannot secure all systems and networks because of the ever-increasing number of internet-connected devices, significant amount of information being shared online, and the extremely sophisticated technology used by cyber-criminals. These new tools present both risks and opportunities for NATO and EU because they can be leveraged by the potential adversaries but could also serve and support NATO. For example, AI technology may increase the number, variety and virulence of cyber-attacks, but can also enable to ability to defend from sophisticated real time attacks with a minimum number of personnel. In that regards, the European Defence Agency (EDA) has the role to support Member States at the project and conceptual level. This entails C2 projects (e.g. ESC2S[1], ECYSAP[2]) and support to shaping the EU Defense initiatives (CARD[3], PESC[4], and EDIDP[5]) along the entire spectrum of capabilities. Based on the preliminary results of these projects, emerging and disruptive technologies for data collection, exploitation and dissemination are expected to have a substantial impact on the transformation of C2 processes and cyberspace operations. New sensor technologies, Big Data technology, cloud computing, AI, and autonomous systems will be used to aggregate more data, at a higher speeds, more accurately, and comprehensively. This will support and speed up decision making. Decision makers will be able to focus on high-value tasks, which due to their characteristics as well as for ethical reasons technically cannot (or shall not) be delegated to machines. These technologies can also be used in modernizing equipment and notably key mission components. This could not only make the sensor to shooter link much shorter and accurate, but also turn each platform into an effective sensor. All operational domains (Land, Sea, Air, Cyberspace, and Space) will be influenced by a drastic digital transformation and modernization. This will notably change our ways to run the intelligence preparation of the battlefield, to develop the Commanders Critical Information Requirements (CCIRs), to approach decision making and to delegate responsibilities. Finally, there is a need a more pragmatic concept to handle more data, quicker and more accurately, to transform cutting edge technology into an advantage on the ground in any Area of Operations in a multi-domain and multinational (combined) environment, including cyberspace.

The fourth point that was discussed was the risk of cyber-attacks to the software/hardware supply chains. A recent example is the Solar Wind long-term intrusion in US networks that can pose a global risk to national critical infrastructures and NATO missions. In the past, most of

1 European Strategic Command and Control System
2 European Cyber Situational Awareness Platform
3 Coordinated Annual Review on Defence
4 Common External Security Policy
5 European Defence Industrial Defence Programme

the software and hardware components used for military applications and critical infrastructures were developed and implemented directly by the military or trusted agencies and companies. Currently, this supply chain depends almost exclusively from a small number of multinational manufacturers which attract the majority of the available European Research and Development (R&D) funds. NATO governments and research entities are not able to supervise the quality of Information Communication Technology (ICT) devices during production and this may result in the proliferation of cyberspace vulnerabilities, which can be and are regularly exploited. Based on these considerations, it is of paramount importance both that NATO and the EU continue to foster multinational cooperation with Allied countries, specifically industries and universities, to promote European laws to oversee multinational companies and mitigate this risk.

The final important point raised during the seminar is the Italian outlook to Cyberspace Operations. In 2020, the Italian Armed Forces established the Joint Command for Network Operations (JCNO), to ensure a robust cyber defense capability for the Italian Defense networks, as well as the capability to plan and conduct cyber operations as part of multi-domain operations. This new three-star command centralizes the responsibility and the chain of command of both the network infrastructure and cyber capabilities. Additionally, the JCNO is actively cooperating with the Cooperative Cyber Defence Center of Excellence (CCD COE) of Tallinn. This Joint HQ cooperates intensively with the Italian Armed Services (Army, Air Force, Navy and Carabinieri) and is fully integrated within the National Cyber Security Committee, chaired by the National Department for Information and Security. Moreover, the JCNO is cooperating with the national industry and academia in the development of several projects, among them a national cyber range.

In conclusion, NATO must protect its freedom of maneuver in cyberspace with existing cyber defensive initiatives, such as the "Military vision and strategy on Cyberspace as a domain of Operations[6]", and the "Integration of Sovereign cyber Effects. The Provided Voluntarily by Allies into Alliance operations and missions (SCEPVA)[7] "), should be expanded to all cyberspace areas, across all the Capability Lines of Development (including Doctrine, Organization, Training, Materiel, Information, Leadership, Personnel, Facilities, and Interoperability). In that regards, the Alliance should also consider to:

- increasing the speed of decision making process by extending the concept of Mission Command based on decentralized decision making and decentralized execution;
- improve CIS/C2 resilience to software and hardware vulnerabilities by developing "Cloud Computing" Infrastructures, Platforms and Software as Services (IaaS, PaaS, SaaS);
- accelerate the development of an Internet of Military Things (IoMT) in conjunction AI enabled command control capability for integrated cyber and kinetic operations;
- increase cooperation with universities and invest additional resources in emerging technology areas including AI, Big Data, Information retrieval, Machine Learning, Machine-to-Machine and Internet of Things (IOT) security;
- improve information sharing and collective understanding of cyber threats;
- reinforce the interaction amongst our respective national cyber defence stakeholders to deepen co-operation and to exchange best practices;
- partner governments and international organizations to be able to attribute the source of cyberspace attacks and request support to implement adequate countermeasures.

While collective discussions about the complex cyber domain are still nascent, we assert that the importance of defensive and offensive cyber capabilities will only grow in importance. The distinguished speakers who provided their enlightening insights are already shaping next year's Cyber seminar, with a projected focus on the "Attribution Dilemma." Our cooperation and collaboration in this area is essential to our nations, the EU, and NATO. NRDC-ITA is looking forward to continuing to support this important discussion.

About the Author

Lieutenant Colonel Gianfranco ELENA has been working as Chief Cyberspace Operations at NATO Rapid Deployable Corps Italy since 2017. He is a senior CISO and CTO with proven leadership experience. He served as signal battalion commander leading 230 IT specialists to accomplish mission-critical projects in overseas operations. He has presided over, developed and implemented many important Electronic Warfare, Cyber Security and Cloud Computing projects in close collaboration with military and civilian organizations (e.g. ENISA, Scottish Government, ESA).

6 MC 0665 - Military Vision and Strategy On Cyberspace as a Domain Of Operations, 2018
7 MCM 0112- Integration of Sovereign Cyber Effects Provided Voluntarily by Allies into Alliance Operations, 2018

er

verywhere apidly

Issue 31 - July 2021

DEEP WATCHING ON CYBER THREAT

nrdc-ita.nato.int

The Magazine of the
NATO Rapid Deployable Corps - Italy