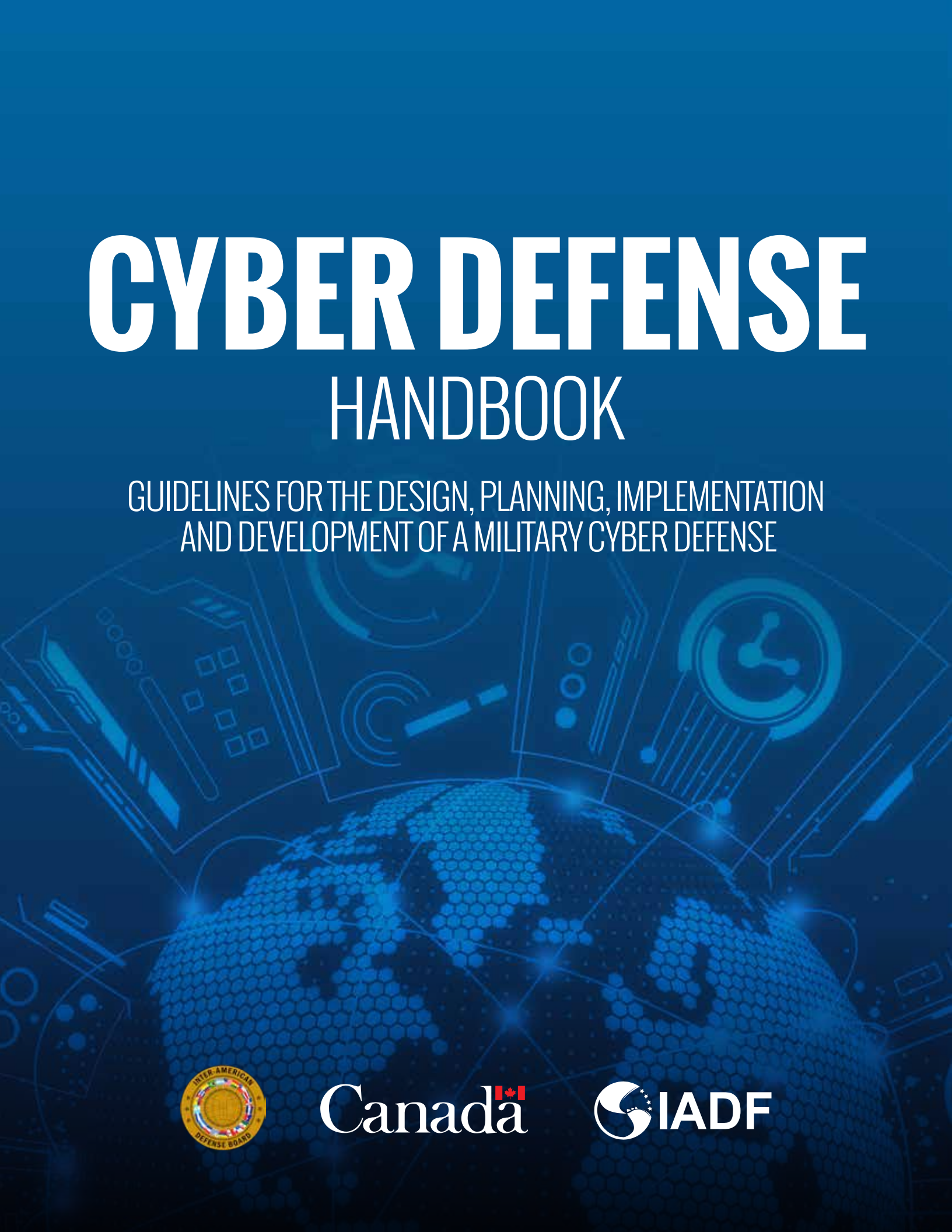
CYBER DEFENSE
HANDBOOK

GUIDELINES FOR THE DESIGN, PLANNING, IMPLEMENTATION AND DEVELOPMENT OF A MILITARY CYBER DEFENSE



INTER-AMERICAN DEFENSE BOARD

Major General Luciano José Penna
President of the Council of Delegates

Brigadier General Juan José Gómez Ruiz
Director General of the Secretariat

Proyect Coordinator

Isabel Niewola
IADB Cyber Defense Program Director

Main Author

Néstor Ganuza

Technical Team

Gonzalo García-Belenguer
Jossele Monroy
Miguel Rego

THIS PROGRAM AND PUBLICATION IS FUNDED BY THE GOVERNMENT OF

Canada

CONTENT

FIGURES

PREFACE

Significant regional and international cooperation around cybersecurity has emerged between governments in the Americas over the past decade, but much of progress has overwhelmingly been focused on civilian institutions. In some countries, where the armed forces play a lead role in cybersecurity, the military has been actively involved in sharing information and best practices with neighboring states. Nonetheless, the military has generally remained outside of the growing regional collaborative framework that has evolved around cybersecurity and cybercrime in the Western Hemisphere.

The Inter-American Defense Board (IADB), supported by the Inter-American Defense Foundation (IADF), has received mandates from the Organization of American States (OAS) on cyber defense and has begun to make significant progress in facilitating communication and collaboration on cyber defense among the Western Hemisphere's security and armed forces.

As the premier organization for military and defense issues in the Americas, the IADB has the opportunity to meaningfully impact policies and strategies, and to facilitate increased regional cooperation. It is in a unique position to bring together military and civilian decision-makers from Latin America and the Caribbean, to enhance the role of military and defense institutions in increasing cybersecurity, reducing the incidence and impact of cyber attacks as well as improving training and information-sharing.

With the support of the Government of Canada, the IADB has launched its Cyber Defense Program, which supports its 29 member countries with capacity-building activities and exercises that will strengthen the Hemisphere's cyber defense policies and capabilities at speed and at scale, individually and collectively. The IADB and IADF are working with existing partners and initiatives so as to enhance and supplement their results.

The military institutions have a direct and pressing interest in bolstering their individual and collective cyber defense capabilities, both to ensure the security of their own military-specific systems, infrastructure, processes, and information, and to be able to contribute to securing broader national interests against growing cyber threats.

The IADB and IADF will continue to further multilateral, bilateral and national cyber defense discussions and serve to inform strategy and decision-making, which will act as a catalyst to strengthen relationships, advance multilateral interests, share best practices, and learn from allies and partners. Cyber defense represents the single greatest shared threat and opportunity for cooperation in the Western Hemisphere.

LIEUTENANT GENERAL LUCIANO JOSÉ PENNA
President of the Council of Delegates
Inter-American Defense Board.

Cyberspace is no longer an "emerging" domain, but a potential theatre of war in which all sovereign nations could be actively engaged on a daily basis. Around the world, state and non-state actors have developed cyber capabilities, both offensive and defensive, that have triggered a re-examination of traditional notions of global power, influence and even warfare.

Today, there is a global dependence on readily available computers and networks for most aspects of governmental, financial, commercial, industrial, and to command and control military operations - a dependence that has introduced both great opportunity and significant risk.

Cyber threats to the security of the Western Hemisphere are becoming more frequent, complex, destructive and coercive. We must adapt to the evolving cyber threat landscape. The Americas require strong and resilient cyber defenses to fulfil critical tasks such as collective defense, crisis management and cooperative security. We need to be prepared to defend our networks and operations against the growing sophistication of the cyber threats and attacks we all face.

Cyber-defense is critical to the conduct of modern military operations. Military cyber infrastructure presents potential single points of failure for operations, training, and activities. Freedom of action within and through cyberspace depends on our ability to protect and defend against accidental, malicious or adversarial action.

Cybersecurity is the foundation of preserving freedom of action in cyberspace. It comprises the application of security measures for the protection of communication, information and other electronic systems, as well as the information that is stored, processed or transmitted in these systems in order to safeguard confidentiality, integrity, and availability. Good cybersecurity sets the conditions for effective operational command and control of military forces.

Since cyberspace is not constrained to a single country, protecting our interests in cyberspace is a team sport. Developing a strong, combined defense against malicious cyber activity requires collective will to coordinate, collaborate and share best practices in the development of cyber forces, and the execution of cyber operations.

This guide is a first step in advancing the development of national cyber forces capable of operating in this new environment, singly and collectively, in defense of our common goals. I encourage all participating nations to review and consider its recommendations closely and look forward to cooperating in cyberspace to secure a safe and prosperous future.

BRIGADIER GENERAL STEPHEN M. LACROIX
Commander, 3rd Canadian Division and Joint Task Force (West)
Canadian Armed Forces

Canada

INTRODUCTION

The continuous transformation of the armed forces to adapt itself to the current strategic scenarios is an essential component of the defense policy of nations. This transformation and adaptation are especially unique in historical moments when a new domain of operations is recognized. This has been the case, throughout history, in the milestones that have incorporated Navy, air force, and cyber force into the armed forces.

The transformation of the armed forces, to adapt to the new current strategic scenario that considers cyberspace as the fifth domain of operations, is occurring unequally in the nations. In general, the development of cyber forces and the art of their use (military cyber defense) is in its initial maturity level.

The purpose of this guide is to offer orientation to realize this transformation and develop a military cyber defense capability comprehensively and methodically, at all necessary levels.

The guide provides an operational model, considering cyber defense a component of joint military operations and therefore aimed at the mission and not yielding to the usual IT systems security-based approach.

The terminology used is mostly military rather than the usual technical terminology, thus reinforcing understanding from a military perspective and facilitating the integration of cyber defense when engaged in joint action with other domain of operations.

The content is organized into nine units (cyberspace, domain of operations, military cyber defense, cyber force, cyber threat, doctrinal principles, cyber ecosystem, legal aspects and standards) to provide a comprehensive approach.

The cyberspace unit analyzes the environment in which cyber defense activities take place; it provides a practical representation that facilitates its understanding, study and use; and it analyzes the main part of cyberspace (the Internet), including the deep and dark web.

The domain of operations unit details all the fundamental components of a military domain of operations from a cyberspace perspective, highlighting its particularities and differences with traditional domain of operations.

The military cyber defense unit brings cyber defense closer to the military art of using cyberspace and military operations in cyberspace (cyber operations), while proposing a cyber operations taxonomy.

The cyber force unit details the aspects to be considered in the process of developing the military force responsible for planning and conducting military operations in cyberspace and the basic capabilities it must have to carry out its tasks successfully.

The cyber threat unit analyzes the global threat landscape and trends, and in particular, the main threat associated with States, advanced persistent threats, and how to fight them.

The doctrinal principles unit analyzes the applicability to cyberspace of the traditional principles of joint operations.

The cyber ecosystem unit puts military cyber defense in context and analyzes relationships with its natural environments, national and international cyber security and the private sector.

The legal aspects unit analyzes the current situation of consensus in the application of international law to cyber operations, both in peacetime and in wartime or peacekeeping missions, and considers those aspects that are most relevant for military cyber defense.
Lastly, cyber defense and cyber security standards are analyzed and assessed.

Definitions and acronyms of the most relevant terms used in the guide are included to provide a better understanding.

DEFINITIONS AND TAXONOMY, A NEED FOR GLOBAL CONSENSUS

Many terms relating to the cyber domain are currently controversial. There is no single globally accepted glossary of cyber-related terms and taxonomy, and therefore, most studies associated with cyberspace and cyber defense are required to prepare their own lists of definitions.

Significant dysfunctions ensue from this lack of global consensus on many issues related to the cyber domain:

a Lack of a common global perception.

The lack of a common global perception of the cyber domain produces different perspectives in the analysis and study of cyberspace, and, in particular, in military operations in cyberspace, the offshoot of which is the formulation of doctrines, definitions and taxonomies with different approaches, which in some cases are incompatible.

b Difficulty understanding the cyber domain.

The confusing–and sometimes contradictory–information about matters regarding the cyber domain hinders decision-making in cyber defense-related issues, which, in many cases, results in decisions that do not fulfill the real need.

c Different organizational structures

The lack of a global consensus multiplies the different visions on how to organize national cyber defense structures, consequently hindering the much-needed national and international cooperation in the cyber defense domain. While some nations have chosen to create a single component command subordinated to the defense staff, some have opted to create a branch within the ministry of defense, a unit that jointly runs cyber defense and CIS, or a cyber defense unit subordinated to the military or national intelligence services.

d Conflict of responsibilities

Different definitions and taxonomies fuel conflicts in the assignment of tasks, causing two concerns: tasks that are left undone due to not having identified the responsible entity clearly and precisely, and tasks in dispute between different organizations, creating conflicts and duplication of efforts and consequently, lack of efficiency.

For all these reasons, it is important to reach a global consensus in the definitions of the most relevant terms linked to the cyberspace domain and, in particular, to cyberspace as a domain of operations.

DEFINITIONS

Advanced Persistent Threat (APT)	An organized group of experts, normally associated with a State, that uses sophisticated knowledge, tools and TTPs (tactics, techniques and procedures) to infiltrate, take control and persist in a third-party network, in order to have access to selected information and gain strategic advantages.
Cyber	Related to cyberspace.
Cyber attack	The deliberate use of a cyber weapon, by a person or automatically, to cause damage to a component of the opponent's cyber space.
Cyber control	The degree of dominance in a cyberspace battle, of one cyber force over an opposing cyber force.
Cyber defense	An organized and prepared capability to fight in cyberspace, which includes defensive, offensive and exploitative activities.
Cyber ecosystem	A system comprising all the components that are related to each other through cyberspace, as well as with cyberspace itself.
Cyber force	1. A military unit specialized in cyberspace combat 2. The ability to carry out offensive actions in cyberspace 3. A set of cyber defense units of the armed forces grouped under one single command 4. In the broadest sense, it is the cyberspace-based military branch, service branch or armed service of a nation.
Cyber key terrain (CKT)	A set of components of cyberspace, in any of its layers (human, cyber-human, cognitive, logical, IT and geographic) that facilitate the activities, operations or functions essential to the mission and the destruction, interruption or impairment of which would generate a significant operational advantage for the adversary.
Cyber operation	A set of military actions that are planned, organized, coordinated and carried out by cyber defense units in order to achieve effects in cyberspace, as well as in the other domain of operations.
Cyber operation	A set of military actions that are planned, organized, coordinated and carried out by cyber defense units in order to achieve effects in cyberspace, as well as in the other domain of operations.
Cyber human	The identity of a cyberspace user in online communities or activities.
Cyber range	A restricted cyberspace area used to train cyber defense units and practice real cyber operations in a safe and isolated environment.
Cyber risk	The probability that a cyber threat exploits a vulnerability to cause damage to an organization's asset.
Cyber security	An organized set of measures aimed at preventing, avoiding and minimizing potential damages to their own networks and information systems.
Cyber situational awareness (CSA)	A representation of the components and events of a cyber ecosystem, at a specific time, place and mission, the explanation of their meaning and the projection of their future state.
Cyber threat	A potential source of damage to any organization's asset that materializes through cyberspace.
Cyber threat hunting	A dynamic and proactive cyber defense process aimed at the detection and isolation of advanced threats that evade the traditional security solutions based on SIEM and perimeter cybersecurity devices (firewalls, IDS, IPS, sandboxing, etc.).

Cyber weapon	Software and TTPs specifically designed to cause damage to a cyber ecosystem component.
Cyber weapon system	A system that integrates different cyber weapons, command and control functions and all the technical support necessary to implement an offensive, defensive or exploitative cyber operation with a specific strategic, operational or tactical objective.
Cyberspace	The notional environment in which communication over computer networks occurs. (Oxford Dictionary).
Domain of operations	The sphere of interest and influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects. (NATO Bi-SC Initial Assessment of Recognising Cyberspace as a Domain).
Hacktivism	The use of cyberspace to carry out civil disobedience, propaganda or proselytizing activities to promote political or social change.
Information system	The set of logical computing resources that facilitate information management for a specific purpose (logistics, command and control, weapons management, financial and human resources, etc.).

CYBERSPACE

001. *Cyberspace* is the conceptual domain where cyber defense activities take place, therefore it is vitally important to have a clear and precise idea of its nature and particularities.

002. According to the Oxford dictionary, cyberspace is "the notional environment in which communication over computer networks occurs." This definition fits the implicit meaning of this guide.

003. Cyberspace is a concept, idea, or notion; it is not a material, physical, visible or tangible space. Since cyberspace is a notion, then no physical or tangible components, such as IT infrastructure, hardware or people, are an intrinsic part of it. Non-tangible components such as information, software or electric power are also not intrinsically part of it.

004. The notion of cyber space is materialized through the interrelation of specific components *(IT infrastructure, software, information, transportation, electric power and people)* providing it with vitality.

005. Cyberspace, the components and their relationships make up the *cyber ecosystem* (para. 524). In practice, the term cyberspace is used to include the components and their relationships, assimilating it to the term cyber ecosystem.

006. Usually, cyberspace is identified with the *IT infrastructure* (computers, servers, wiring, IT devices and hardware), which would seem to make it more understandable; but this cyber-IT identification carries the great danger of digressing from the true purpose of cyber defense.

007. This *cyber-IT misperception* is a source of conflict between cyber defense units, in charge of planning and conducting military operations in the cyberspace domain of operations, and CIS or Signal units, in charge of providing cross-domain telecommunications service to all domain of operations.

008. *Information* is not an intrinsic part of cyberspace, but cyberspace is an ideal environment to manage it (create, present, process, store, transport, share, and delete). Cyberspace, however, is not the only environment where information can be tackled.

FIGURE 1. CYBER ECOSYSTEM

009. *People,* individually or in organized groups, are not intrinsic part of cyberspace, just as they are not part of any other domain (land, air and sea). People create and modify cyberspace; they perform activities, functions and operations in cyberspace, but they are not part of cyberspace.

010. Finally, two components that keep cyberspace alive are important to mention: *software and electric power*. These are the two basic components to maintain cyberspace's vital signs.

011. The IT component that describes cyberspace is made up of two main parts: *the Internet and isolated systems* (networks, systems and storing devices not connected to the Internet).

012. In the military world, both the Internet and isolated systems are crucial: the Internet provides global connectivity and massive access to information, and the isolated systems provide an effective environment to manage classified information and to carry out activities that require a high level of confidentiality and isolation.

013. These two characteristics, global connectivity and isolation, are not exclusive of each part of cyberspace (the Internet and isolated systems), since confidential and isolated environments can be created on the Internet and isolated networks can be implemented with high connectivity. But they are not the natural environments.

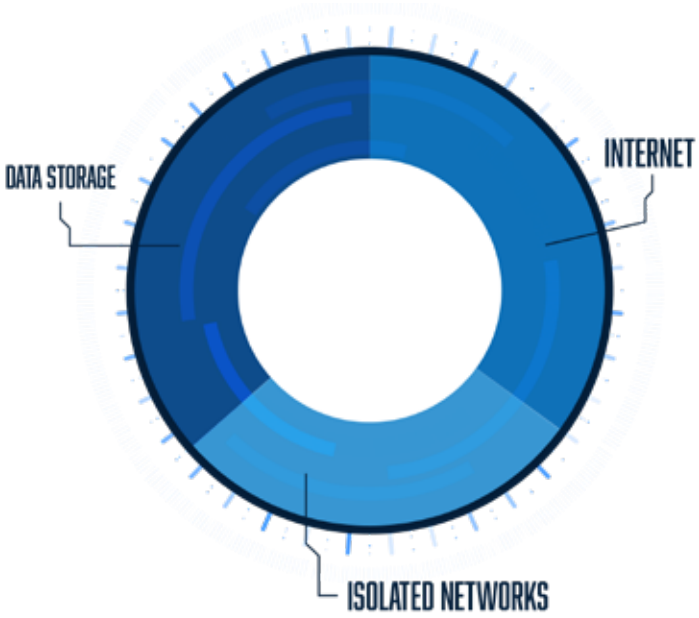


FIGURE 2. CYBER ECOSYSTEM IT ELEMENT

014. Both parts, the Internet and isolated systems, are paramount in a national cyber defense framework, considering that global connectivity is essential in order to have extensive access to information and for national and international cooperation; and isolation and confidentiality are fundamental in the activities related to operations and research and development.

Cyberspace layers

015. From a practical and operational point of view, it is helpful to assemble the components that interact in cyberspace in different layers *(human, cyber-human, cognitive, logical, IT infrastructure and geographic)* to facilitate the assignment, organization and distribution of activities, functions, services and responsibilities.

016. Different activities are performed in each of the layers, relating to different means, processes and professional profiles.

017. The representation of cyberspace in layers follows a logical process whereby humans generate knowledge that is processed on information systems implemented in IT networks located in specific places of the geography.

FIGURE 3. CYBER ECOSYSTEM LAYERS

018. The *human layer* comprises the physical people that carry out their activity in cyberspace.

019. The *cyber-human layer* involves the cyber people or online identities (identity of a cyberspace user uses in online communities or activities). Humans and cyber humans may or may not coincide.

020. The *cognitive layer* is made up of knowledge built by people's interaction with information systems and specific knowledge of cyberspace expressed in doctrine, norms, standards, procedures, guides, etc.

021. In the cyberspace domain of operations, *cyber situational awareness (CSA)* is a critical component of the cognitive layer.

022. The *logical layer* is basically composed of information systems. An information system is understood as a set of logical computing resources that facilitate information management for a specific purpose (logistics, command and control, weapons management, financial and human resources, etc.).

023. In the logical layer, digital identities–information used by information systems to represent an entity–are assigned. This entity can be a person, organization, application or device.

024. The *IT layer* is made up of all the physical network devices that enable data transport. Hardware, systems software, wired or wireless networks, interconnection devices, connectors, servers, computers, peripheral devices, perimeter security devices, etc.

025. The *geographic layer* is made up of the physical areas corresponding to the traditional domain of operations (land, sea, air and space) accommodating the IT infrastructure and the people who support cyberspace.

The Internet

026. *The Internet* is an open and independent network of networks that operates worldwide and is run by non-profit organizations (companies, universities, governments, and others) working together to meet their needs.

027. Physically, it uses a part of the total resources of currently existing public telecommunications networks.

028. Technically, it works using two basic protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP).

029. The Internet is the fundamental part of cyberspace. In any military operation in cyberspace, it is essential to identify critical Internet points that may affect the development of the mission; in particular, internet service providers (ISPs) and internet exchange points (IXPs).

030. An *Internet service provider (ISP)* is a commercial organization (in many cases, the telecommunications operators) with permanent connection to the Internet, that sells temporary connections to customers.

031. An *Internet exchange point (IXP)* is a physical infrastructure through which internet service providers (ISPs) exchange Internet traffic.

032. Internet interconnection is conducted through a three-tier hierarchical structure.

033. The top level *(Tier 1)* is for a small number of ISPs that connect directly to each of the other Tier-1 ISPs and to a large number of Tier-2 ISPs.

034. Any Tier-1 ISP has global connectivity; therefore, it can reach any Internet point in the world without having to pay any fee for traffic exchange.

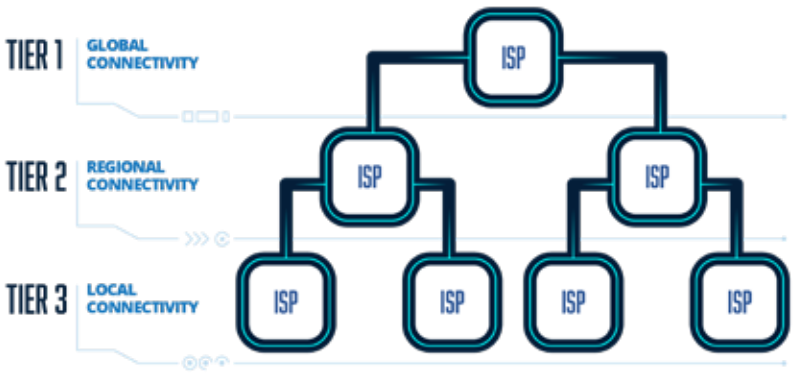


FIGURE 4. INTERNET HIERARCHY

035. *Tier-2 ISPs* typically have regional or national coverage, connecting only to a few Tier-1 ISPs, and in some cases, must pay a fee for traffic exchange.

036. *Tier 3 ISPs* have limited coverage, connecting through Tier 2 ISPs and having to pay to transmit traffic on other networks.

037. The Internet is a *distributed system* and, consequently, no single political power can make a significant impact on the entire global Internet network. However, the risk that a nation may get disconnected from the internet is real. In fact, some countries have developed systems that make it possible to isolate their country's internet from world servers and thus guarantee national operation, even in the case of international cyberspace conflict.

038. A country's *disconnection from the Internet* is a potential strategic risk with serious consequences. Due to the phenomenon of globalization, most of nation's services depend on external connections, therefore, even if there is total national connectivity, an isolation from the Internet would have serious internal repercussions.

039. The *degree of risk* that a country get cut off from the Internet depends directly on the number, robustness and resilience of the national internet connection points (ISPs and IXPs).

040. The number of Tier-1 ISPs and IXPs per country is small and thus are critical assets for national cyber defense.

041. In addition to having a sufficient number of ISPs and IXPs to avoid the risk of internet isolation, the ISP/IXP infrastructure must be under the control of different entities, both public and private, since the decentralized government of the Internet is its greatest strength.

042. *The hidden web (deep and dark web)* is a collection of websites

FIGURE 5. INTERNET EXCHANGE MAP BY TELEGEOGRAPHY

and databases that standard web search-engines (Google, Yahoo, Bing) cannot index and, therefore, is an ideal environment to carry out traceless activities.

043. Unlike the surface web, the information and traffic that runs on the deep web cannot be easily found or observed by users. The hidden web is a set of closed communities with access restricted only to authorized members. Communities, such as scientific, academic, or governmental, may have lawful interests or they may be criminal organizations with malicious purposes.

044. The hidden web is characterized by *anonymity*, using specific browsers such as TOR (The Onion Router). Nothing that is done on the hidden web can be tracked or associated with the originator's identity, unless that originator wills it.

045. The hidden web is part of the overall Internet that must be considered in cyber defense, both for protection against malicious activities and, also, for performing legitimate confidential or dangerous activities that require an isolated environment.

CYBERSPACE DOMAIN OF OPERATIONS

046. At the NATO Warsaw Summit 2016, allies *recognized cyberspace as another domain of operations.* Specifically, the paragraph 70 of the communiqué states that "Cyberattacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise 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. It will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success."

047. NATO, in fact, did nothing more than confirm a fact: cyberspace is being used daily by armed forces of many States as yet another capability an operation commander can avail himself of to produce strategic effects on the adversary.

Domain of operations

048. A *domain of operations* is the sphere of interest and influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects. [1]

049. For a given domain to be qualified as a domain of operations, it must meet six criteria:
1. Requires unique capabilities to operate in that domain.
2. Is not fully encompassed by any other single domain.
3. Is characterized by a shared presence of friendly and opposing capabilities.
4. Is able to exert control over an opponent trough influence and dominance.
5. Provides opportunities for synergy with other domains.
6. Provides asymmetric opportunities across domains.

050. Cyberspace undoubtedly meets all six criteria and is therefore qualified as a domain of operations.

051. Cyberspace, as a domain of operations, is an environment where specific military operations (cyber operations, para. 206) are conducted. These cyberoperations can produce direct cyber effects (para. 145) and indirect physical effects in traditional domains.

052. In order to produce the desired effects, the cyber force (para. 221) must have freedom of action and be able to exercise control over the opponent (cyber superiority, para. 168).

FIGURE 6. CYBERSPACE DOMAIN OF OPERATIONS

053. The ultimate purpose of cyber operations is for the cyber effects to support mission accomplishment. Therefore, cyber defense capabilities and their potential effects must be considered throughout the entire life cycle of joint operations planning and conducting.

Nature of cyberspace

054. Cyberspace has some singularities *(artificiality, imperceptibility, dynamism, ubiquity, immediacy, transversality)* that distinguish it from the other domains and therefore requires special capabilities to operate in it.

055. Cyberspace is an *artificial*, man-made environment, and, as such, modifiable thereby. In fact, cyberspace is acquiring a new dimension as new technologies and services emerge. The original Internet of the web and email have little to do with the current web involving social media, cloud and the Internet of Things.

056. Cyberspace is physically *imperceptible, invisible and intangible,* which makes it even more difficult to understand and interpret than traditional domains. This difficulty makes it yet more challenging when defining and developing military capabilities and procedures to operate in it.

057. Cyberspace is a *dynamic and changing environment* that requires permanent monitoring, continuous cyber situational awareness updating and flexible planning.

058. Cyberspace is *ubiquitous and immediate*. An action in one place can have almost immediate effects anywhere else in the world. Unlike the other domains, in most cases, it is unnecessary to deploy cyber defense forces in the geographical environments where the effects are to be produced.

059. *Cyberspace has borders,* that is, it has a perimeter that separates an internal area from an external area and which allows an owner or authority to control the movements between them.

060. Effective border protection in cyberspace scales poorly, compared to other domains. Certainly, effective access control in cyberspace can be established when selecting entities authorized to access a given area of cyberspace, but as this area broadens, access control weakens.

061. States have effective mechanisms to carry out selective access control of their national sovereign land, sea and air spaces. Nevertheless, carrying out a similarly effective control in the national sovereign cyberspace is currently unfeasible, despite attempts by some countries to create their own sovereign internet.

062. Cyberspace is *cross-domain.* In reality, it behaves like a supra-space with imposing presence and influence over the other domains. This transversality means that cyberspace must be especially taken into consideration in all joint aspects (doctrine, operations planning and development, organization, etc.)

FIGURE 7. CROSS-DOMAIN CYBERSPACE

Cyber Key Terrain

063. The *Cyber Key Terrain (CKT)* is the set of cyber ecosystem components, in any of its layers (human, cyber-human, cognitive, logical, IT and geographic) that facilitates the activities, operations or functions that are essential to the mission and the destruction, interruption or impairment of which would award a significant operational advantage for the adversary.

064. In any cyber operation, as well as in any joint operation, it is necessary to identify the CKT components, study and assess their vulnerabilities, probability of being attacked and impact on the mission if sustaining an attack.

065. In most cases, trying to protect all the CKT components is not feasible, therefore the CKT list must be prioritized and updated on a regular basis, to subsequently carry out a protection plan according to prioritization.

066. The CKT component identification and protection process should be done in the same way that key terrain identification and protection is done in land, sea and air domains.

067. The cyberspace layer model facilitates the CKT component identification process.

068. *The CKT components in the human layer* are the people whose knowledge is considered essential for the operation and protection of all the components on the CKT list.

069. *The CKT components in the cognitive layer* are the data, information or knowledge, which, if disclosed to the adversary, would seriously jeopardize the mission or if manipulated by the adversary, would create mistrust in the information systems essential to the mission.

070. *The CKT components in the logical layer* are the information systems (including command and control, weapons, and navigation systems) that, if controlled or interfered with by the adversary, would seriously jeopardize the mission.

071. *The CKT components in the ICT layer* are the IT networks components that, if controlled or interfered with by the adversary, could lead to denials of service or degraded performance of mission critical services.

072. *The CKT components in the geographic layer* are the sites where critical IT components are located (data processing centers, network control centers, IT security operations centers, internet exchange points, critical internet service providers, submarine cable infrastructure, etc.) and, if physical destroyed, could jeopardize mission accomplishment.

073. *The protection of national submarine cable infrastructures* and their land connection points (points of presence and landing stations) must be considered a strategic priority in the national cybersecurity framework, since they are the main global communications platform. In particular, it is estimated that more than 95% of all transoceanic digital communications are carried out on the submarine cable infrastructure, since it is faster and cheaper than satellite infrastructure.

074. *Submarine cable sabotage* is a complex operation, but it is now considered a standard operating procedure for intelligence services of some States, as well as suspicious naval maneuvers carried out near strategic submarine cable routes and land connection points albeit raising concern among potentially affected countries.

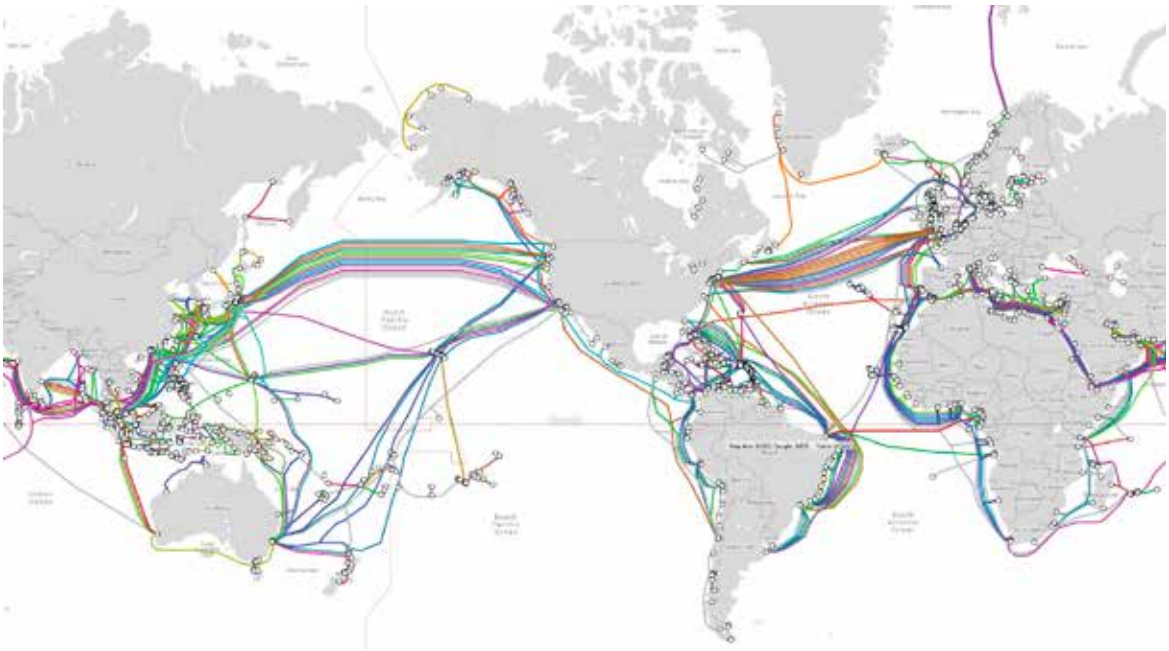


FIGURE 8. SUBMARINE CABLE MAP BY TELEGEOGRAPHY

Cyber risk

075. *Risk management* is basic in cyber defense and is a part, intentionally or involuntarily, of all the phases of a decision-making process. A decision, in most cases, is the result of the comparison of risks associated with the different feasible options.

FIGURE 9. CYBER RISK

076. *Cyber risk* is the probability that a cyber threat will indeed exploit a vulnerability to cause an impact (damage) to an asset that has a specific value and criticality. In short, it is an indicator obtained from two factors: probability and impact.

077. The probability of sustaining a cyber attack is higher as the threat capability and its interest in the potential victim's assets increase.

078. The probability of sustaining a cyber attack is higher as the number of the targets' vulnerabilities increases, since the threat's activity becomes easier and more profitable.

079. The *impact* is higher as the value of the attacked assets–for the organization–increases.

080. The impact is higher as the criticality of the attacked assets increases. That is, when other important assets for the organization depend on the attacked assets.

081. In the context of cyber defense, the risk to consider, above all, is the risk to the mission due to cyber threats. In other words, how a successful cyber threat materialization can jeopardize the mission.

FIGURE 10. MISSION CYBER RISK

082. It is necessary to minimize the risks of the cyberspace components when their operation is essential for mission accomplishment. These are the components of the cyber key terrain list.

083. Cyber risk is managed through a seven-phase systematic process:

1. Identify and prioritize the CKT components according to their potential impact on the mission in case their operation is impaired.
2. Identify and evaluate the vulnerabilities of the CKT components.
3. Identify the potential cyber threats that can jeopardize the mission and assess their capability.
4. Identify the assets of highest interest to the threat, either because they are valuable or useful to the threat or because they are those with the highest impact on the organization, which is the threat's goal.
5. Identify the risks by carrying out a methodological analysis using a specialized tool and methodology (MAGERIT[2] /PILAR[3] , CRAMM[4], OCTAVE[5] , etc.).
6. Define and prioritize mitigation measures for identified risks.
7. Prepare and implement a risk management plan.

FIGURE 11. RISK MANAGEMENT

084. Cyber risk management is a *dynamic process* where the identification and assessment of new threats, vulnerabilities and assets must be a continuous task and when a significant change occurs, they must feed the process, generating a new analysis.

085. There are four traditional ways to mitigate risk: *avoidance, reduction, sharing and retention.*

086. *Cyber risk avoidance* implies not carrying out the activity that may entail a cyber risk.

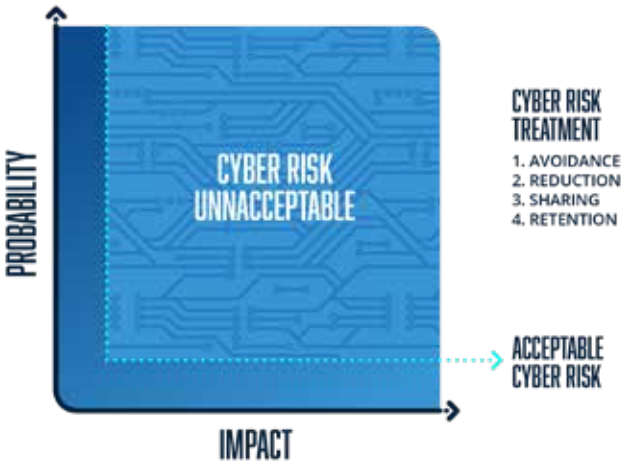


FIGURE 12. CYBER RISK TREATMENT

087. Although risk avoidance seems a somewhat crude measure, in reality, it is a fairly common in cyberspace. Examples are the implementation of black or white lists in the access to certain web pages or the selective restriction for access to information (need to know).

088. *Cyber risk reduction* involves reducing either the severity of the loss or the probability of the loss occurring, for example, by implementing cybersecurity measures, hiring cybersecurity services, investing in cyber deterrence, or implementing contingency plans.

089. *Sharing or transferring cyber risk* involves distributing, with a third party, the burden of loss or the measures to reduce cyber risks, for example by taking out insurance as a post-event compensatory mechanism or establishing a collaboration agreement with other organizations potentially affected by same cyber risks.

090. Cyber risk retention involves accepting the loss of a cyber risk when it occurs. It means doing nothing to reduce the probability or the impact. In practice, all the cyber risks that are neither avoided, reduced or shared are retained.

091. Cyber risk retention is a viable strategy for extreme cyber risks; that is, if the probability of a very severe loss is small or if the cost of insurance is so great that it would hinder realizing the organization's objectives. An example is the risk that a data processing center will be destroyed by an earthquake in an area with little seismic activity.

Cyber tactics

092. The military use of cyberspace is a new field that still has a lot to define and explore, but that does not mean that it is starting from scratch. The traditional forms of defense and use of force, in their essence, do not vary; what is needed is to find the way to carry them out with means and procedures especially adapted to cyberspace.

093. *Traditional military tactics* from traditional domains such as *reconnaissance, force concentration, infiltration, surveillance, ambush, and fire and movement* are also applicable in cyberspace.

094. *Reconnaissance* is a requisite activity prior to planning and conducting a cyber operation with the main purpose of identifying the topology and vulnerabilities of the adversary cyberspace in all its layers.

095. *Force concentration* in cyberspace can be done in two ways, quantitatively or qualitatively.

096. Quantitative concentration of cyber forces refers to the concentration of numerous human resources (public resources, universities, population), most without a high technical or professional qualification, focused on the same target or task.

097. An example of quantitative concentration is when a State uses a large number of people on staff (armed forces units, university students, etc.), without necessarily a high-level professional qualification in the field of cyber defense, to pursue systematized instructions developed by a group of experts focused on concrete targets. It is a profitable strategy for high population States that can afford to spend the effort of many people on a single task (e.g. many people trying to find an access point in a system until one of them succeeds).

098. Another variant of quantitative concentration is when a State takes advantage of a hot or unstable social or political situation to convince and encourage a disgruntled population group to carry out malicious activities in cyberspace, concurrent in time and against the same target, following clear, simple and precise instructions, generally seeking denial of service effects.

099. *Qualitative concentration* is when a large number of experts and technological and economic resources are concentrated in an organized and coordinated manner, creating a special cyber defense unit.

100. Qualitative concentration is a more common strategy than quantitative and is generally carried out by groups (APTs) associated with States, either organically or covertly.

101. *Infiltration* refers to clandestine access to networks of adversaries with the purpose of affecting their systems or information or with the intention of taking surreptitious control of them. It is a fundamental tactic in APTs or cyber espionage.

102. *Surveillance* refers to monitoring their own networks, internally and at the perimeter, in order to detect malicious actions or suspicious behaviors. It is one of the main activities of the security operations centers (COS, CERTs, CSIRTs, para. 340/342).

103. *Ambush* in cyberspace is carried out mainly through honey pots, honey nets, cyber deception platforms or weaponized decoys.

104. *Honey pots* are virtually isolated (although simulating connectivity) network devices with fictitious activity (although simulating real activity), deliberately vulnerable (not excessively so that they appear real), aimed at attracting the attention of attackers (so that attackers believe they have successfully infiltrated the network but, in fact, they are actually being analyzed in an isolated environment) in order to analyze their tactics, techniques and procedures (TTPs), as well as trying to frustrate them and abandon the attack.

105. *Honey net* is a network composed of honey pots. Currently, the implementation of cybersecurity measures based on honey net technologies are not sufficient protection against experienced cyber attackers (APTs), therefore the use of other more advanced and proactive technologies such as cyber deception platforms is required.

106. *Cyber deception platforms* are sophisticated, dynamic and automated honey nets that are located in real logical environments, with the ability to detect, analyze and tackle, in real time, zero-day[6] and advanced cyber attacks.

107. Cyber deception technology considers cyber attackers' TTPs and integrates with other cybersecurity technologies to provide cyber situational awareness, early threat detection and threat intelligence. It is especially useful for cyber threat hunting.

108. Cyber deception platforms are more at risk of interfering with the operation of real networks, so the technological solution must be carefully selected and tested before being implemented.

109. *Weaponized decoys* are electronic files or pieces of software, simulating information of interest to a potential cyber attacker, having preinstalled embedded malware designed to be activated on the cyber attacker's network if exfiltrated.

110. *Fire and movement* in cyberspace refer to the need to design cyber attacks so that once they have caused the desired effect, they leave no trace of the attacker and the TTPs used, so that they cannot be attributed or reusable.

Human factor

111. In cyberspace, unlike other domains, two types of people coexist: the physical human (real identity) and the cyber human (online identity).

112. *Cyber human* or online identity is the person as shown in cyberspace or the identity that a cyberspace user establishes in online communities or activities. It can be created and managed by a physical person or automatically by tools designed ad hoc.

113. A cyber human can have one or more real or fictitious identities associated with it and, in turn, a person can be associated with, or control, one or more cyber humans. In many cases, it is difficult to identify whether a cyber human corresponds to the person, group or entity that the human claims to be.

Cyber weapons

114. *A cyber weapon* is a piece of software and TTPs specifically designed to cause damage to a cyberspace component and may have physical effects in the traditional domain of operations.

115. Like traditional weapons, a cyber weapon is the means (cyber attack vectors) that allows the transfer of the payload (malware, exploits[7]) to the targets (adversary networks and systems). By extension, a cyber attack is considered the combination of vector and the payload.

116. Cyber attack vectors or techniques are numerous; some of the most common are phishing[8], spear phishing[9], spoofing[10], pharming[11], sniffing[12], watering hole[13], DoS[14], DDoS[15], MitM[16] and SQL injection[17].

117. Often, notions that do not cause misunderstandings in traditional domains do create confusion in cyberspace. This is the case of cyber attacks and cyber weapons that are usually assimilated. For example, in the physical world no one doubts that a pistol is a weapon and that an attack occurs when a person makes specific use of the pistol against a target. In cyberspace, it is the same; a cyber weapon is a means and a cyber attack is the deliberate use of that means by a person or automatically.

118. Cyber weapons are designed to cause different severity of damage (destruction, denial, degradation, disruption, and exfiltration) to targets in cyberspace or other domain of operations.

119. Usual *targets* of a cyberweapon are information (destruction, denial, degradation, interruption and exfiltration), IT systems and network functionality (destruction, denial, degradation, interruption), reputation (destruction, degradation), matériel (destruction, degradation), facilities (destruction, degradation) and people (destruction, degradation).

120. *Information* is usually the main target of high-level organized groups (APTs). Even though they have the ability to disable the compromised system, they prefer not to affect its operation in any way, in order

FIGURE 13. CYBER ATTACK TARGETS

to remain unnoticed as much as possible to exfiltrate information. Cyber weapons like Flame[18] have been especially designed for cyber espionage.

121. It has been demonstrated that ciber weapons, the effects of which extend beyond cyberspace and which may affect equipment, facilities and people, undeniably exist. Examples of such cyber weapons are Stuxnet[19], Duqu[20] or Black Energy[21].

122. A cyber force (para. 221) must have an appropriate arsenal (para. 409) that allows it to make legitimate use of force when allowed by law.

123. A cyber weapon can actually have multiple purposes. It is the set of different cyber weapons together with ad hoc procedures, command and control tools and specifically qualified personnel that enables the development of a cyber attack with a specific target.

124. A cyber weapons system integrates different cyber weapons, command and control functions and all the technical support necessary to develop an offensive, defensive or exploitative cyber operation against a specific target.

125. According to the extent of the effects, the cyber weapons system can be strategic, operational, or tactical.

Cyber attack

126. A *cyber attack* is the deliberate use of a cyber weapon, by a person or automatically, to cause damage to a component of the opponent's cyber space, which may have indirect effects in the other domain of operations.

127. The commander of an operation must consider all available capabilities to achieve the desired effects. Therefore, the Commander must consider traditional and cyber attacks and physical and cyber effects.

128. There is no strict one-to-one correspondence between cyber attacks and cyber effects and between physical attacks and physical effects since a cyber attack can produce physical effects and a physical attack can produce effects in cyberspace.

129. In a *joint operation,* all possible combinations of attacks must be considered: attacks originating in one domain and with a target in the same domain (Earth-Earth, Sea-Sea, Air-Air, Space-Space, Cyberspace-Cyberspace) and attacks originating in one domain and with a target in another domain (Earth-Sea, Earth-Air, Earth-Space, Earth-Cyberspace; Sea-Earth, Sea-Air, Sea-Space, Sea-Cyberspace; Air-Earth, Air-Sea, Air-Space, Air-Cyberspace; Space-Earth, Space-Sea, Space-Air, Space-Cyberspace; Cyberspace-Earth, Cyberspace-Sea, Cyberspace-Air, Cyberspace-Cyberspace).

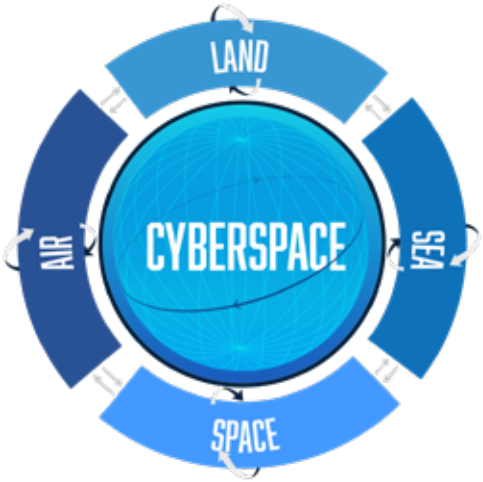


FIGURE14. TYPES OF ATTACKS

130. To detect and repel a cyber attack it is necessary to know how it works and its development process.

131. The *Cyber Kill Chain*[22] framework is a model based on seven phases (reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives) aimed at systematizing the identification and prevention of cyber intrusion activities and thus facilitate the detection of an attack and understanding its TTPs (tactics, techniques, and procedures). Obviously, it can be used, also, to coordinate and organize cyber attacks.

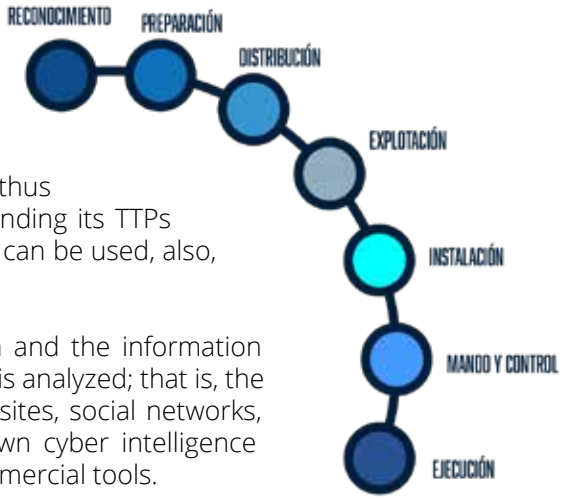


FIGURE 15. CYBER KILL CHAIN™ BY LOCKHEED MARTIN

132. In the *reconnaissance phase,* the target is chosen and the information necessary to plan and implement the cyber attack is analyzed; that is, the existing public information on the target (on websites, social networks, etc.) and that has been made available by its own cyber intelligence services, using open source tools (OSINT[23]) or commercial tools.

133. Reconnaissance includes passive activities (public network monitoring, obtaining information from open sources, etc.) and active activities (i.e., social engineering) aimed at obtaining information about the target (cyber defense capability, vulnerabilities, network topology, credentials, emails associated with the target, etc.)

134. In this initial phase, the attacker fingerprints the target to obtain its networks and systems topology, organizational structure, relationships, communications, and affiliations and to identify its vulnerabilities, both technical and human, to later be able to infiltrate and exploit the network.

135. This phase can take a long time, but the time spent in this phase is worth it since the more you know, and the better the knowledge about your opponent, the higher the probability of a conducting successful cyber attack.

136. In the *weaponization phase,* the information obtained in the reconnaissance phase, the detailed knowledge of their own resources and the types of effects desired serve to plan the cyber attack, select the most effective tools and assemble the payload (appropriate malware and exploits for exploiting known or unknown vulnerabilities) in the attack vectors (pdf or word documents, compromised web domains, spoofed emails, usb memory devices, etc.).

137. It is necessary to use new, modified or redesigned malware to reduce the probability of detection by traditional security solutions that identify known signatures.

138. In the *delivery phase,* the payload is transferred to the target environment. It is a critical moment since it is the moment in which the target is contacted and some of the attempts can be detected and rejected, so it is very important to design the attack to leave as little trace (fingerprint) as possible.

139. In addition, it is necessary to monitor the effectiveness of the intrusion attempts to focus on the most profitable ones.

140. In the *exploitation phase*, the payload is activated by exploiting a vulnerability in the target environment (an application, the operating system, or the users themselves) and running malware on the system. Installing malware in the target environment requires end-user involvement by inadvertently enabling it (payload).

141. In the *installation phase,* malware is consolidated in the target system and a connection to the outside is established with the installation of a remote access Trojan or a back door and thus maintain persistence within the environment.

142. In the *command and control phase,* the attacker, taking advantage of the external communication channel and consolidated malware in the target environment, takes surreptitious control of part of the system to perpetrate new attacks commanded from an operations coordination center established for this purpose.

143. At this point, traditional cyber defense based on firewalls, intrusion detection systems (IDS), sandbox, and security information and event management (SIEM[24]) are not effective. Only cyber defense based on cyber threat hunting (para. 478) would be effective together with a well-organized group of experts with the necessary authority to carry out mitigation and reaction measures.

144. In the *actions on objectives phase,* the attacker, once having taken control of the target's system, performs actions to achieve the desired effects (cyber effects, para. 145) and takes advantage of the system's control to spread to other systems and objectives, which would imply performing the cyber kill chain again.

Cyber effects

145. *Cyber effects* are the damage or impacts produced by cyber attacks. They can be grouped into two main groups, noisy and silent. Each of them has advantages and disadvantages for both the attacker and the victims. It is necessary to consider all type of effects in any cyber operation (defensive, exploitative and offensive).

146. *Noisy cyber effects* are the impacts that are clearly perceptible by the victim, such as denial or degradation of service, unavailability of information to authorized users, perceptible modification of web content, encryption ransomware in order to prevent access and even physical destruction of equipment or facility.

147. Usually, noisy cyber effects cause significant operational, economic or reputational losses, although short lived, since in most cases the effects are reversible if there is an effective operations continuity plan (para. 290).

148. Noisy impacts are often quite noticeable, raising alarm and consequently triggering a reaction in the victim that can lead to an investment of additional cyber defense resources to reverse the situation and prevent recurrence.

149. The cyber kill chain of noisy cyber attacks is usually short lasting. The reconnaissance and weaponization phases are usually short because these attacks tend to not be very sophisticated. The delivery, exploitation and installation phases are usually short because they do not need to avoid early detection given that the effects themselves raise the alarm. The command and control phase is usually short because it does not need an external communication channel. The actions on objectives phase is short because the time between the first attack and detection is immediate.

150. *Silent cyber effects* are the impacts that go unnoticed by the victim, such as information exfiltration, non-conspicuous modification of information and web content, impersonation, credential theft, network monitoring, etc.

151. Silent effect cyber attacks seek persistence, that is, to have control as long as possible. Consequently, originators take great care not to leave a trace and they combine periods of activity with periods of inactivity, which are sometimes very long. In addition, they camouflage their activity under the usual parameters of the victim's activity so as not to attract attention.

152. Usually, silent effect cyber attacks cause significant long-standing operational, economic or reputational losses, although the organization, in many cases, may not be aware of this.

153. In most cases, silent effect cyber attacks are not detectable by traditional cyber defense means (threat detection), therefore advanced cyber defense (threat hunting) is required.

154. The cyber kill chain of silent effect cyber attacks are usually long lasting. The reconnaissance and weaponization phases usually take long because silent cyberattacks are very sophisticated and require careful preparation. The delivery, exploitation, installation and command and control phases are usually long because early detection must be avoided by all means. The actions on objectives phase, in particular, is usually very long; that is, the period from the first attack until the victim detects the cyber attack usually takes years and, in many cases, the period from detection until the victim manages to totally eradicate the attacker's action can also take years.

155. Silent effect cyber attacks are extremely dangerous because, for years, the victim does not perceive the loss of operation and competitiveness.

FIGURE 16. CYBER EFFECTS

Military cyber deterrence

156. *Military deterrence* is one of the main strategic lines of the armed forces. It is, as Sun Tzu (544-496 BC) said, "to win without fighting."

157. An effective military deterrence capability must meet three requirements: capability, determination, and declaration.

158. Deterrence is based on the capability of a potential victim to inflict greater harm than the expected benefits by a potential threat, should an attack be triggered.

159. Military capability must be ready to be used at the right time and place through a continuous training, and evaluation.

160. *Determination* is the firm will to use force, if necessary, to anticipate, prevent or respond to an attack.

161. *Declaration* is the public announcement of the capability and determination to be clearly known to potential adversaries.

FIGURE 17. DETERRENCE

162. It is neither necessary nor advisable to provide more details on capability than necessary. Flaunting the extent of the effects of the capability should be enough (publishing news, reports or studies, or performing public cyber exercises, maneuvers, etc.).

163. In cyberspace, deterrence is not perceived as clearly as it is in traditional domains because of the difficulty in attributing the origin of the cyber attack. In other words, retaliation must occur against a known attacker and whose authorship is attributable without any doubt, and this, at present, is a complex matter since cyber attackers usually conduct their assaults through compromised third-party networks that are not aware of it.

164. The complexity of attribution in cyberspace makes *passive deterrence* (having a cyber defense robust enough to make the effort and resources consumed by a potential cyber attack unprofitable) more relevant.

165. Military deterrence is understood from a comprehensive perspective where retaliation against a cyber attack does not necessarily have to be carried out through a cyber defense capability, but through any type of military attack; in short, the aim is to stay free of attacks of any kind.

166. Therefore, *comprehensive military deterrence* is the declared determination to make use of any available military capability (conventional, nuclear and cyber) if necessary.

FIGURE 18. COMPREHENSIVE DETERRENCE

Cyberspace control

167. The control of the spaces of influence in combat in traditional domains (land, sea and air) is one of the fundamental requirements to gain the necessary freedom of action and avoid interference from adversaries. In the cyberspace domain of operations, this need (cyberspace control) is equally necessary.

168. *Cyberspace control* is the degree of dominance of the confrontational cyberspace of one cyber force over an opposing cyber force.

169. There are 5 levels of cyberspace control: cyber supremacy, cyber superiority, cyber parity, cyber denial, cyber incapability.

170. *Level 1 (cyber supremacy)* is reached when there is complete control of the confrontational cyberspace. Adversary cyber forces are powerless to conduct any effective interference. Its own freedom of action is unmitigated while the opponent's is minimal.

FIGURE 19. CYBERSPACE CONTROL

171. *Level 2 (cyber superiority)* is reached when there is a more favorable position over the opponent in the confrontational cyberspace. The freedom of its own action is greater than the opponent's.

172. *Level 3 (cyber parity)* is reached when there is exclusive control over its own networks and systems. The two cyber forces have similar freedom of action and capability to interfere in each other's area.

173. At *level 4 (cyber denial),* the opponent is in a more favorable position in confrontational cyberspace. Its own cyber force can continue to operate, but improperly. Its own freedom of action is less than the opponent's.

174. At *level 5 (cyber incapability),* the opponent has complete control of the confrontational cyberspace. Opposing cyber forces can fully interfere. Its own freedom of action is minimal while the adversary's is total.

175. To reach level 1 and 2, it is necessary to have *defensive and offensive capabilities.* With defensive capabilities exclusively (activity in its own networks), a cyber force can only aspire to level 3 (cyber parity) if also, the opposing cyber force does not have offensive capabilities. Otherwise it can only aspire to level 4 or 5.

Options in combat

176. To carry out a correct assessment of the best option to use in combat to achieve the desired effects, the commander must assess, among all the available capabilities (traditional and cyber), the one that best meets, at least, the criteria of efficacy, efficiency and less risk to its own forces and third parties.

177. *Criterion for efficacy* refers to the action that causes exactly the desired effects.

178. *Criterion for efficiency* refers to the action that requires the least economic, human and material resources.

179. *Criterion for risk to its own forces* refers to the action that puts its own people, means and facilities at less risk.

180. *Criterion for risk to third parties* refers to the action that produces less collateral damage, mainly civilian victims and those not involved in the conflict.

181. The weight of each criterion on assessment is established by the operation commander, although, obviously, the first criterion is effectiveness, since it makes no sense to choose an option that does not create the desired effects. Once all the effective options have been chosen, the action that best meets the remaining conditions based on operational, economic or legal imposition criteria (the case of risks to third-parties or its own forces) would be selected.

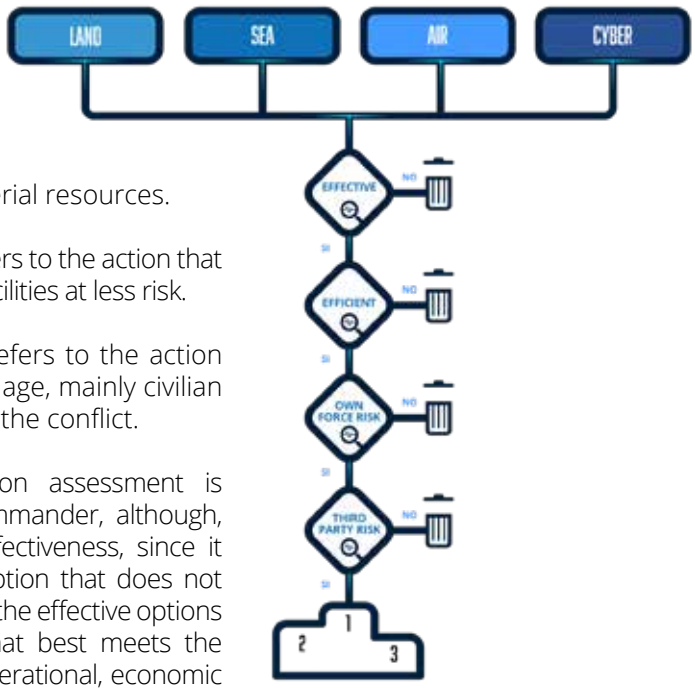


FIGURE 20. OPTIONS IN COMBAT

182. In many cases, the option that best meets all four conditions is an action in cyberspace. If an operation commander had cyber defense capabilities available and the option that best met all four requirements were an action in cyberspace, then it would be difficult to understand, from an operational, ethical and legal point of view, why that commander did not choose the cyberspace option over the traditional ones (para. 645).

Asymmetry in combat

183. *Asymmetry in combat* in cyberspace is the disparity or disproportion between the resources necessary to cyber attack and those necessary for cyber defense, which means that, in many cases, the resources necessary to plan and conduct a cyber attack are less than those necessary to defend against that cyber attack.

184. Asymmetry in combat is graver in cyberspace than in the other domains due to reasons related to exposure surface, resources, legal framework, technology, personnel and identity.

185. *The defender's exposure surface* is greater than the surface used in the attack. Defenders must prepare their defense against any type of attack on any part or component of their networks, while attackers will limit their activity to those components that make the attack possible by focusing on exploiting a reduced number of vulnerabilities.

186. In most cases, an organization invests more resources (financial, material, technical, and human) in defending its networks and systems than attackers do to intrude upon or cause them to malfunction. Although this is usually the case, it is not so in all cases. For example, to develop a STUXNET-type cyberattack requires the investment of an enormous amount of resources, only available to States or large corporations.

187. *Legal framework* favors attackers. Cyber attackers can evade national legislation by conducting cyber attacks from compromised networks located in third countries, while defenders are subject to compliance with the national legislation where the infrastructure is located.

188. The lack of international and bilateral agreements and the lack of a consensual and binding international legal framework on cyber defense makes it difficult to prosecute cyber attackers.

189. The defender, in most cases, cannot make use of *cutting-edge technology,* either for reasons of budget constraints or for technical reasons, since an organization cannot expose its defenses with technologies that have not yet been extensively tested. On the other hand, the attacker may risk using an unproven emerging technology and discard it if it does not produce the desired effects (trial and error).

190. Defense technologies and tools are often better known to the attacker than attack technologies and tools by a defender, because defense technologies and tools tend to last over time to pay off the economic investment, while an attacker continually tests new technologies and tools to surprise the defender.

191. The defense of networks and systems usually requires specially qualified *personnel* in many cybersecurity aspects. On the contrary, in many cyber attacks, a limited group of experts is needed to develop instructions and coordinate the action of a larger group of individuals with little qualification in cyber defense.

192. The attacker generally knows the *identity* of the defender and the defender's environment (organization, system, activity, functions, location, etc.) while the defender usually does not know the attacker.

193. In the cyber operation planning process, it must be taken into account that the *profitability* of an offensive action may be greater than that of a defensive action, as the saying goes, in some sports "an attack is the best form of defense."

MILITARY CYBER DEFENSE

194. Military cyber defense is the organized capability of the armed forces prepared to fight in cyberspace. It is the base and foundation of the national cyber defense that can also rely on other State powers (political, economic, diplomatic, etc.) when the occasion requires it. It includes defensive, exploitative and offensive activities.

Cyber defense and related disciplines

195. The concept of cyber defense is often misunderstood and assimilated to other overlapping disciplines, making the design and development of a cyber force and its effective integration into the armed forces and national cyber defense difficult.

196. Disciplines especially related to cyber defense are cyber operations, computer network operations (CNO), cyber security, information operations, electronic warfare, psychological operations and strategic communication. The best way to differentiate them is to study their purpose.

197. *Cyber operations* focus primarily on the mission; on causing effects that facilitate mission objectives. Cyber defense is a broader concept that includes cyber operations as the central axis, along with all the command, technical, logistical and administrative capabilities necessary for planning and conducting them.

198. *Computer network operations* is an obsolete concept that can be assimilated to cyber operations, but focused exclusively on cyber effects, not considering the physical effects on people or facilities.

199. *Cybersecurity* focuses on the protection and recovery of its own IT networks and systems.

200. *Information operations* focus on information, primarily on achieving information superiority and influence. One of the aims of cyber defense is to protect its own information and affect the adversary's, but cyber defense has many more objectives.

201. *Electronic warfare* focuses exclusively on the electromagnetic spectrum, in any activity that involves the use of the electromagnetic spectrum and directed-energy weapons to control the spectrum, attack an opponent, or protect against attacks across the spectrum.

202. *Psychological operations* focus on people and are often very helpful and provide support to cyber operations.

203. *Strategic communication* focuses on communication and, naturally, cyberspace is possibly the best way to manage communication. But it is not the only one.

204. All these related disciplines have aspects that fit into or support cyber defense, although using different means and different professional qualifications. Therefore, it is necessary to consider them in cyber defense and establish ways of coordination and collaboration.

205. Cyber defense is a discipline that is specialized in the use of cyberspace and therefore it can be helpful in achieving the objectives of the related disciplines. The opposite is also true, the related disciplines can be helpful to cyber defense.

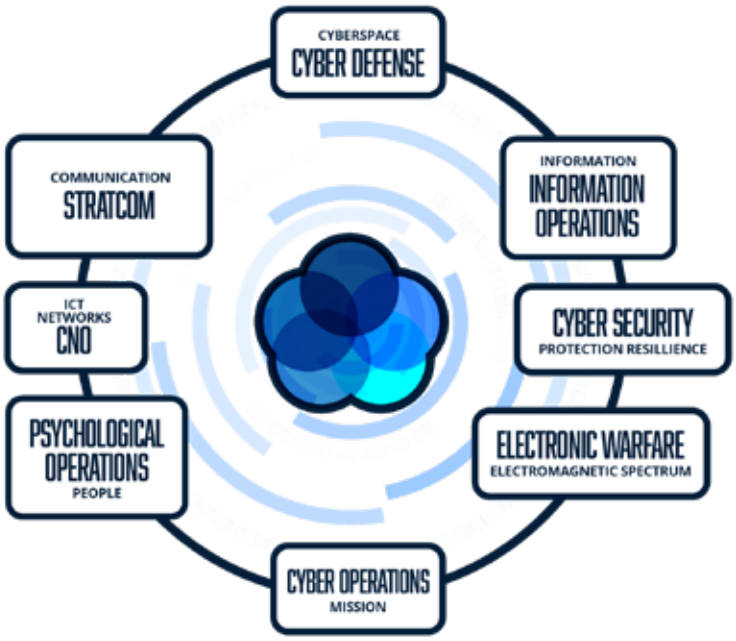


FIGURE 20. CYBER DEFENSE AND RELATED DISCIPLINES

Cyber operations

206. *Cyber operations* are military actions planned, organized, coordinated and carried out by cyber defense units in order to achieve effects in cyberspace, as well as in other domains.

207. There are six types of cyber operations, according to their nature, objective and environment in which they take place: passive defensive, active defensive, passive exploitative, active exploitative, response, and offensive.

208. *Passive defensive cyber operations* run on their own networks and focus exclusively on prevention, protection, and resilience of their own cyberspace. No specific actions are taken against an adversary or a third party.

209. *Active defensive cyber operations* use intrusive or offensive techniques (ethical hacking, penetration testing, etc.) on their own networks (authorized by networks' authority) aimed at searching for vulnerabilities and risks and assessing the security level of their own cyberspace.

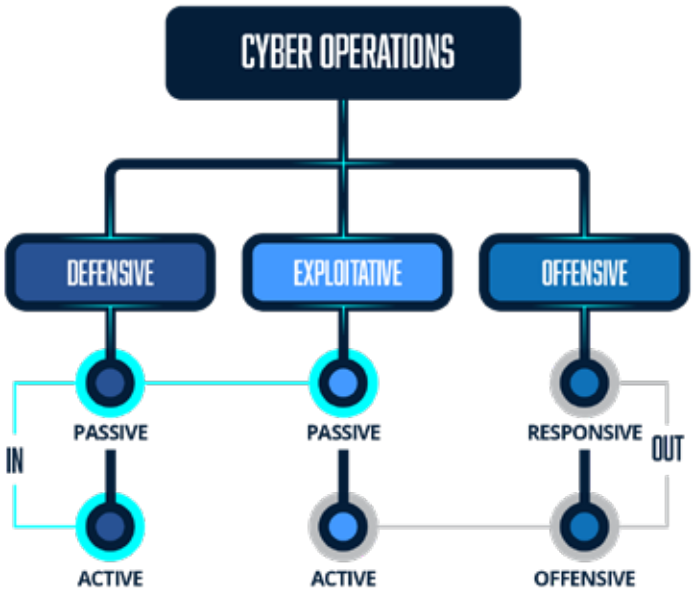


FIGURE 21. CYBER OPERATIONS

210. *Passive exploitative cyber operations* are non-intrusive cyber operations, carried out on their own networks or public networks, aimed at obtaining information necessary for planning and conducting defensive and offensive cyber operations or other conventional operations.

211. *Active exploitative cyber operations* are intrusive cyber operations, carried out on the networks of adversaries or third parties, aimed at obtaining information necessary for planning and conducting defensive and offensive cyber operations or other conventional operations.

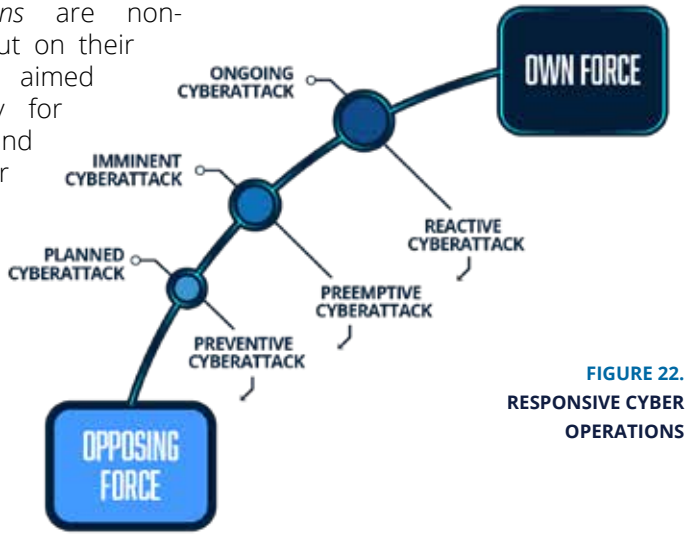


FIGURE 22.
RESPONSIVE CYBER OPERATIONS

212. *Response cyber operations* are offensive cyber operations carried out on the networks of adversaries or third parties, in order to prevent, anticipate or react to cyber attacks on their own networks.

213. Depending on the moment in which response cyber operations are executed, in relation to the adversary's intention, they can be preventive, preemptive or reactive.

214. *Preventive cyber operations* are response cyber operations conducted against an adversary to avoid a cyber attack that, according to information obtained from their own intelligence or allies, is planned and will occur in the near indeterminate future.

215. *Preemptive cyber operations* are response cyber operations conducted against an adversary to avoid a cyber attack that, according to information obtained from their own intelligence or allies, will occur imminently.

216. *Reactive cyber operations* are response cyber operations conducted against an adversary to repel an ongoing cyber attack.

217. Some contemporary studies equate preventive attacks with aggression, and therefore characterize them as illegitimate. Other studies consider that when an alleged adversary appears to begin confirmable preparations for a possible attack in the near future, the attack cay in fact be considered to have already begun.

218. *Offensive cyber operations* are carried out in the framework of a declared conflict, on the networks of adversaries or third parties, with the purpose of causing a cyber-effect or a physical effect.

219. *False flag cyber operations* are offensive cyber operations that are carried out covertly with the intention of blaming an innocent third party.

CYBER FORCE

220. In order to fulfill the mission of protecting national interests, the armed forces of a State must have the capability to face the threat wherever it occurs, on land, sea, air, space or cyberspace. For this reason, they must have proper military capabilities to combat in all domain of operations, adapted to the nature of the domain, trained and prepared for use when and where they are needed and properly organized to carry out their activities, functions and operations in coordination with other domains.

221. *Cyber force* is the set of the armed forces units, organized under the same single command, responsible for planning and conducting military operations in cyberspace.

222. The current global strategic scenario includes cyber threat, not only as a present threat in any declared conflict, but also as a persistent threat present also in peacetime or in undeclared conflicts. Consequently, the armed forces must have a cyberspace force designed, organized and prepared not only to be activated in case of conflict but to be in permanent combat activity, which gives the cyber force special relevance compared to the land, sea and air forces.

223. Developing a force for effective use in an emerging domain, the doctrinal maturity level of which is very low, requires careful, complex and flexible planning; a legal framework that supports its missions and tasks; a doctrine that serves as a reference for its organization, preparation and employment; an organization adapted to its functions and tasks; specialized personnel; permanent training; adequate command, operational and technical capabilities for combat in cyberspace; secure facilities especially adapted to its tasks; and all of this subordinated to a single command, ensuring maximum effectiveness and efficiency.

224. In the broadest sense, the cyber force is considered the cyberspace-based military branch, service branch or armed service of a State.

Development planning

225. Planning the development of a cyberspace force must be carried out with care and caution since the lack of knowledge and experience of the domain can lead to erroneous decisions that, once established and consolidated, can be very difficult to eradicate or modify. Therefore, lessons learned from other countries should be taken into account and adapted to national circumstances.

226. *Cyber force development planning* is a comprehensive process where all aspects (political, organizational, operational, technical, logistical, administrative and legal) must be considered, since decisions on one aspect may affect others.

227. Planning must be *flexible* because the lack of maturity of the new domain will often pressure the organizations into making decisions that, once established, could be considered unsuitable. Therefore, the planning itself must include mechanisms that will expedite changes in direction, procedures and objectives.

228. When a force is developed for use in an immature environment, the first planning exercise should not be considered definitive, but the preparation should continue in a *cyclical process,* in such a way that after implementing the plan's actions, it must be evaluated in order to assess alignment with the objectives, and accordingly, the planning should be modified and the cycle started again.

229. In the early years of a cyber force, annual or biennial *development plans* can be laid out detailing strategic objectives, lines of action and resources to achieve the objectives. Once the cyber force is consolidated, longer-lasting development plans can be formulated, although given the dynamic nature of cyberspace, it is not convenient to prepare development plans exceeding five years.

Legal framework

230. To guarantee the legitimacy of the missions, responsibilities, tasks, activities and actions of the cyberspace force, its constitution must be secured by a legal norm at the highest possible level, no less than a ministerial decree.

231. The norm should include, at a minimum, the scope, mission, tasks, organization and subordination of the cyber force.

Doctrine

232. The armed forces have a *traditional doctrinal framework* that establishes the fundamental principles, concepts, and guidelines for their organization, preparation, and employment in the land, sea, and air domains, as well as in the joint domain. The cyber force, as part of the armed forces, also needs a specific doctrine to guide its organization, preparation and employment in the cyberspace domain.

233. Due to the dynamic nature of cyberspace and the low maturity level of the cyber space domain of operations, the *doctrine of the employment of a cyber force* may require revisions and modifications more regularly than traditional doctrines, and the guidelines established in it may require increased flexibility.

234. Cyberspace is *cross-domain* with respect to the rest of the domain of operations, being present in them and influencing or supporting their action. Therefore, it is also necessary that cyber defense capabilities be considered in the doctrine of the traditional domains, as well as in the joint operations doctrine.

235. *Cyber defense doctrine* establishes criteria, references, principles and procedures related to all operational aspects within the cyber force, in the context of the armed forces and at the national and international levels.

236. Doctrine is to be understood as a *complete body of documents* that facilitates the organization, preparation, and employment of the armed forces in cyberspace. This set must include, at least, the military cyber defense vision of the chief of defence, the concept of cyber defense, the doctrine for the employment of the cyber force, the operating procedures for each type of cyber operation, technical instructions, guides, recommendations and good practices of cyber defense activities and the integration of cyber defense in other consolidated doctrines.

237. International collective defense organizations such as NATO have a significant responsibility in the formulation of doctrine that serves as a reference to neighboring nations. However, NATO's level of maturity in relation to the cyber defense doctrine is insufficient for current national needs, which forces nations to generate their own doctrine, which could lead, in the future, to the coexistence of doctrines with a different approach that would hinder multinational and international cooperation in cyber defense.

238. The cyber force itself must promote the drawing up of cyber defense doctrine necessary for its operational effectiveness and for the required understanding of cyber defense by other involved actors, thus eliminating areas of conflict or uncertainty.

Organization

239. The traditional way of organizing military capabilities to fight in a traditional domain of operations is through a higher unit *(military branch or service branch)* that brings together all the specific capabilities of each domain, that is, the army, the navy and the air force. They are divided into three main components: the general staff, in charge of advising and supporting the commander and planning operations; the force, in charge of conducting the operations; and force support, in charge of providing all the operational, logistical and technical support necessary to carry out the operations.

240. When a cyber defense unit is created, the lack of consolidated cyberspace domain doctrine and the small size of the unit (a new unit usually begins small) has fostered the trend to fashion it within the organization of another already established domain. In the long term, this produces confusion and misunderstanding, because cyber defense units are then considered to perform just another function (cyber defense) in the land, sea and air domains, comparable to any other of the traditional functions (command and control, intelligence, maneuver, fire, information, civil-military cooperation, protection and logistical support) and disregard its true nature as the force responsible for military actions in a different domain of operations: cyberspace. Therefore, it is advisable, regardless of the size of the unit, to centralize all cyber defense units in a higher unit as a service branch articulated in its three main components (general staff, force and force support) which will facilitate the natural evolution of the cyber force.

241. The level of *technical knowledge* required of the cyber force personnel is high, but this is not exclusive to the cyberspace domain; it is also required in other domains. However, the military staff (tip of the iceberg) should be oriented predominantly to the command, organization, management and coordination responsibilities that fundamentally require *operational knowledge* and leave the technical responsibilities to associated bodies (part of the iceberg that is underwater) such as public and private consultancy services, cybersecurity and IT professional services and academia.

FIGURE 23. CYBER FORCE

242. These associated bodies should feel they are part of the cyber force as well, and for this reason, organizational structures, collaboration agreements and contracts that facilitate this *loyalty* must be defined.

Personal

243. *Cyber defense personnel* should be viewed as critical, operational, permanent, dedicated, and with a long-term payback period. In addition, due to its great potential, special attention should be paid to voluntary reserve in the field of cyber defense.

244. Cyber defense personnel are a *critical resource*. The knowledge required by cyber defense tasks is also useful in many private sector activities. A significant portion of key cyber defense personnel, once they have acquired a high level of experience and knowledge, will be tempted to leave the military and joint the private sector in a higher paying position.

245. The foreseeable resignation by some expert personnel compels cyber defense units to be extremely careful and vigilant with the knowledge gained, ensuring that it is always documented and shared, so that, if talent departure cannot be avoided, at least the *knowledge will remain.*

246. Cyber defense personnel must be considered, for all intents and purposes, *combatant* personnel. All the tasks and responsibilities related to cyber operations in the three facets, defensive, exploitative and offensive, are combat actions, just as they are in the other domains.

247. Cyber threat operates not only in wartime but also in peacetime and in undeclared conflicts. If we add to this the fact that cyber attacks come from anywhere in the world, this means that there will be no reduction in malicious activity due to time zones, working hours or vacation periods, therefore a *24x7x365* cyber defense service is a must.

248. Cyber defense personnel should be considered *exclusively dedicated* to cyber defense throughout their professional careers. Cyber defense is a highly technical discipline and operationally complex, which is related to a domain of operations, therefore, cyber defense personnel must remain throughout their military career in the cyberspace domain to guarantee its effectiveness, in the same way that land, naval or air personnel do. It should be avoided, by all means, to consider cyber defense personnel as personnel from other domains (land, sea and air) who, with some basic training, can perform temporary cyber defense responsibilities.

249. Cyber defense personnel have a *long-term payback period*. In order to achieve the combat readiness level required by their position, cyber defense personnel require superior operational and technical knowledge, gained by a significant investment in training and time. For this reason, in order to "amortize" the investment and be able to obtain an optimal performance from the staff, the cyber defense positions must be defined in such a way that they guarantee a minimum occupation of five years.

250. *A volunteer reservist* is a citizen who wishes to contribute, on a voluntary and temporary basis, the abilities and knowledge gained, in the different missions carried out by the armed forces. This contribution is materialized by engaging with the Ministry of Defense, signing a commitment that entails an active temporary period in military units.

251. In the traditional domains (land, sea and air), volunteer reservists usually carry out their activity in the facilities of the assigned unit, for a limited continuous period per year (usually between 1 and 3 months) and the units themselves provide the reservist with the uniform, equipment and weapons necessary for the performance of the assigned activity.

252. Cyberspace has some particularities that make it suitable for the military reserve, unlike the other domains, but it is necessary to move from an onsite to an online model that maximizes the characteristics of cyberspace and cyber defense to secure effectiveness and efficiency, speed up activation, improve reservists performance and lighten the logistical and administrative burden on units.

253. The cyber reserve online model has the following *advantages*:

- The cyber reservist does not necessarily have to carry out the activity in the facilities of the assigned unit; the individual can take advantage of telecommuting, working from home or the workplace.
- The cyber reservist does not necessarily have to carry out the activity in the facilities of the assigned unit; the individual can take advantage of telecommuting, working from home or the workplace.
- The cyber reservist can carry out the work with the reservist's own means, without the need for an official uniform and means, thus freeing the unit from having to supply the standard official provision.
- The cyber reservist can be assigned to a specific project (based on professional experience) instead of a unit.

254. Despite the fact that the process is based on an online model, the physical link with the unit should not be overlooked and short-term activities (meetings, events, exercises, etc.) that require the physical presence of the reservist in the unit facilities or the physical contact with his colleagues must also be carried out to achieve a stronger loyalty to the unit.

255. Assigned activities and tasks must be carefully selected so that they are perceived by the reservists as a *contribution to National Defense.*

Training

256. To cope with the complexity of cyber defense-related activities and the rapid evolution of cyber defense-related technology, cyber force personnel must receive special and continuous training.

257. Cyber defense training is based on a permanent process of individual training, collective training of cyber defense units and awareness at all levels (end users, cyber defense personnel and senior leaders), defined and conducted through specific annual programs based on the training needs of each position and unit.

258. *Individual training* is aimed at all individuals in the cyber force units in order to provide them with the appropriate skills that enable them to effectively perform the tasks assigned to their position.

259. The cyber force must define the *training path* of each position, establishing the position-access skills degree and certification (level required to be assigned to a position) and the combat readiness skills degrees and certification (level required to keep the position) that must be achieved in a given period of time.

260. The cyber force must study the percentage of time that each individual must dedicate to regulated training during their workday. Depending on the type of activity, the percentage of time dedicated to training is different, but a *20-60 rule* could be considered a reference, that is, all cyber defense personnel must dedicate at least twenty per percent of their time to training and no one can exceed sixty percent. In specific periods, these margins can be exceeded, but at the end of a global calculation (generally related to the duration of the development plan, annual, biennial or five-year) the margins must remain as noted.

261. *The individual training program* must detail, for each cyber force position, the training path considering all aspects (operational, technical and administrative), all levels (tactical,

operational, strategic and political) and it must foresee the necessary resources to carry it out. In addition, the program must define the evaluation and certification criteria for each position.

262. *Collective training* is aimed at cyber defense units in order to train and practice shared, coordinated and organized use of different and supplementary individual skills to achieve the same effect or objective.

263. *Cyber exercises* are standard practice; internally, within the cyber force, and in the national and international context. Cyber exercises have two fundamental purposes: to train individuals in collective tasks and to evaluate and, where appropriate, certify the preparedness degree of units.

264. It should be noted that the two purposes, *training and evaluation,* are often incompatible. The target audience of a training-oriented cyber exercise must comprise individuals (not experts) who are suitable to learn and make the most of the practices; while the target audience of an evaluation-oriented cyber exercise must be made up of the regular staff of the unit to be evaluated.

265. *A collective training program* includes technical and procedural cyber exercises, at all levels of command, in all its facets (defensive, exploitative and offensive) for all cyber defense units, and the definition of the evaluation and certification criteria for each unit.

266. A collective training program must also consider the integration of cyber defense in joint military exercises and in other domains, and it must foresee and encourage participation in cyber exercises at national and international levels.

267. The most common cyber exercises are defensive-technical, offensive-technical and procedural.

268. *Defensive-technical cyber exercises* focus on training in defensive techniques against complex real-time cyberattacks; on garnering experience that is not usually acquired in regular work; on the evaluation or comparison of units; on testing new technologies; on coordination and cooperation between units from different organizations (for example cyber force teams with other military branches, police, national critical infrastructure protection, etc.) and on talent attraction. They are carried out on a cyber range, in which real networks and systems are set up, real techniques and tools are applied; and all this framed in fictitious situations and scenarios based on probable real cases.

269. The most common defensive-technical cyber exercise is based on a model of five types of teams: white team, green team, yellow team, red team and several blue teams.

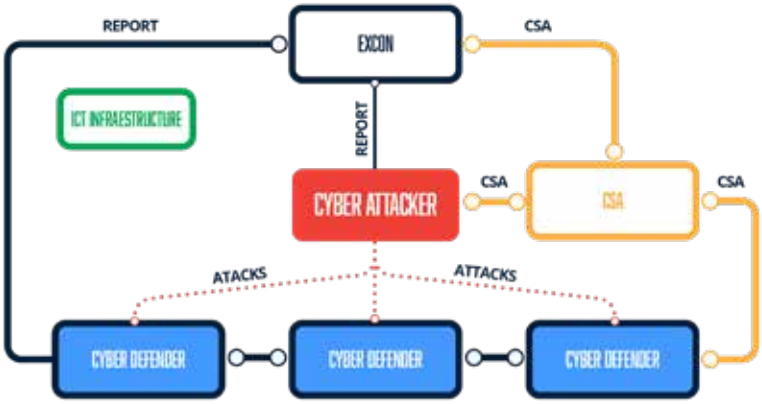


FIGURE 24. CYBER EXERCISE

270. *The white team* is in charge of the cyber exercise management, events inject management, assessment and rating of participants, communications between teams, evaluating blue and red team reports and user and media simulation.

271. *The green team* is in charge of the design and implementation of the IT infrastructure and the management of the cyber range.

272. *The yellow team* is responsible for developing and distributing cyber situational awareness (CSA).

273. *The red team* is in charge of planning and implementing cyber attacks against blue teams and providing data to the yellow team for the preparation of the CSA. In those cyber exercises rating the blue teams, the cyber attacks must be balanced in such a way that each blue team receives cyberattacks that are comparable in amount, time and complexity.

274. *The blue team* is the target audience. It is in charge of planning and executing the defense against the red team's cyber attacks, coordinating and cooperating with other blue teams, providing data to the yellow team for the preparation of the CSA and preparing the technical, legal, forensic, and media reports.

275. In small organizations that cannot afford a full-blown cyber exercise with five teams, they may choose to develop a *blue-red-purple model* (where the purple team is responsible for encouraging and facilitating cooperation between the red and blue team) or by a purple model (where the purple team performs the functions of the red and blue team). These models are not properly cyber exercises since their purpose is not training, but rather the analysis and assessment of the organization's cybersecurity level.

276. *Offensive-technical cyber exercise*s focus on training in offensive techniques against robust and dynamic defenses; on the acquisition of experiences that are not usually attained in regular work; on testing new technologies; and on talent attraction. They are developed in a cyber range, in which real networks and systems are implemented and real techniques and tools are applied; and all this framed in fictitious situations and scenarios based on probable real cases.

277. *Procedural cyber exercises* aim to raise awareness among senior leaders and train them in decision-making; to coordinate and collaborate among agencies responsible for national cybersecurity issues and crisis management; and to validate and verify the effectiveness of cyber defense/security procedures and standards. They are developed in debates where members of different teams discuss optimal solutions to fictional challenges during crisis situations, with the help of a facilitator who guides the participants through one or more scenarios or cases.

278. *Awareness-raising activities* address three types of audiences: high-level audience (senior leader handling sensitive information, interesting for cyber threats), general audience (IT systems end users) and cyber defense-specific audience (cyber force personnel) with the purpose of alerting them about cyber threats and cyber risks and promoting responsible behavior in cyberspace.

279. Effective awareness must consider four aspects: the message, message retention, implementation of the measures, and assessment of compliance.

280. The *message* must be clear, appropriate to the target audience and easily distributed to each individual in the target audience.

281. The message must be designed in such a way that once it reaches the recipient, the recipient is able to assimilate it, understand its usefulness for the organization, understand how to implement it and remember the moments and situations that require putting it into practice.

282. *The awareness program* addresses the three main types of audience (senior leaders, end users and cyber force personnel) in a differentiated way, defines the mechanisms for monitoring and assessing compliance with awareness measures, and establishes the criteria for measuring the effectiveness of the implemented measures.

Command capabilities

283. The cyber force must have capabilities aimed at facilitating decision making, such as planning and advice, cooperation, representation, knowledge management, lessons learned, financial service and legal service.

Planning and advice

284. As in any military unit, the cyber force must have a group of experts in fundamental operational cyber defense aspects (personnel, intelligence, operations, logistics, plans, CIS, training, resources and finances, influence and cooperation) together in a General Staff or Headquarters. This staff is responsible for advising the commander to facilitate decision-making, plan all the activities related to fundamental operational aspects, distribute plans, guidelines and orders, and monitor fulfillment.

285. The *General Staff* prepares specific plans for each operation, as well as the cyber force development plan, the operations continuity plan, the communications plan and all the necessary sector plans (training and awareness; recruitment, motivation and loyalty; financial and gaining resources; intelligence, cooperation, etc.).

286. *Cyber operations planning* should be performed following a standard military planning methodology to facilitate support for operations in other domains, and support and integration in joint and combined operations.

287. *A development plan* is the main plan of the cyber force. With it, the cyber force commander establishes the purpose (the permanent reason for the unit's existence), the mission (the primary objective to be achieved upon complexion of the plan), and the strategic vision (way and conditions to achieve the mission); in addition to all the details necessary to accomplish the commander's intention, such as specific objectives, courses of action, resources, roles and responsibilities, and time frames.

288. During immaturity periods, when the full operating capability (FOC) has not yet been reached, the development plan should be short term (annual or biennial). Once the FOC is reached, the development plan usually lasts 4 or 5 years. Three different FOCs can be considered to be progressively reached (first, the defense FOC, then the exploitation FOC and lastly, the response FOC) when it is necessary to efficiently manage limited resources.

289. The development plan is the main document of the cyber force; it is the reference that guides all activities, responsibilities and tasks, and it is the most effective way to unite personnel, make efforts converge and align results.

290. *The operations continuity plan* contains the technical, human, procedural and organizational measures to recover and restore critical operations that have been disabled or interrupted by a cyber attack.

291. The standard process for preparing an operations continuity plan is based on three phases: threat identification, critical service identification and definition of cyber defense measures.

292. The *cyber threat identification phase* serves to analyze the four general cases (known threat and known response; known threat and unknown response; unknown threat and known response; and unknown threat and unknown response), and to identify and classify the most likely and dangerous threats.

293. In the *known threat/known response case,* cyber defense measures necessary to deal with a specific cyber threat (known TTPs and impact) are known.

294. In the *known threat/unknown response case,* the cyber threat TTPs and potential impacts are known, but the right cyber defense measures to deal with them are not known. It is necessary to experiment with possible solutions and build collaborations with organizations that may have solutions.

295. In the *unknown threat/known response case,* contingency situations are analyzed, anticipating probable impacts, where the measures to recover from them are known, but the causes that produce them are unknown.

296. In the *unknown threats/unknown response case,* a mechanism is established to expeditiously organize a group of experts who can advise in real time on the appropriate reactive measures to unforeseen situations in which the cyber threat TTPs are unknown and reactive measures are not planned.

297. In the *critical services identification phase,* the services, operations, processes, systems, etc. the interruption or disablement of which may lead to an unacceptable lack of operation for the organization should be identified, and the impact measurement criteria that should trigger an automatic or human response should be established.

298. In the *measures definition phase,* all the preventive (data backup systems, backup SOC, etc.) and reactive measures necessary to recover from the expected impacts should be defined, to react to unforeseen impacts and to anticipate unknown threats (cyber threat hunting).

299. *The communications plan* establishes the official position of the cyber force in all the particularly sensitive matters (offensive operations, intelligence operations, organization, resources, capabilities, missions, etc.), identifying the situations in which information can be made public and how and who can deliver information.

300. The communications plan also establishes the form, the way and the responsible entity to report on serious ongoing incidents.

Cooperation

FIGURE 25. COOPERATION

301. *Cooperation,* in all its facets, whether international, national, with the industrial and academic sector, with citizens and internal cooperation within the cyber force, is an essential activity to achieve and maintain solid cyber defense.

302. *International cooperation* is especially relevant in cyber defense due to the ubiquitous nature (attacks can originate from anywhere in the world on compromised networks) and the anonymous nature (without a recognized signature) of cyber attacks, which require the involvement of other countries to identify the origin of the cyber threat and to deliver an effective response.

303. To procure strong international cooperation, it is necessary to establish bilateral agreements with other cyber forces in the geostrategic environment and to actively participate in the collective cyber defense of international defense alliances.

304. In order to make effective *bilateral cooperation agreements,* it is necessary, first of all, to build mutual trust to facilitate a balanced exchange of information, so that neither party feels at a disadvantage with respect to the other in terms of the quantity and quality of the information received vis-à-vis that delivered.

305. Military cyber defense is the main capability of the government of a nation to implement national cyber defense as part of the defense policy, which, in coordination with the other instruments of national power, contributes to national security. It is not always clear whether a cyber threat or a cyber attack is the responsibility of military cyber defense, national cyber defense or national cyber security. For example, in order to avoid a cyber attack targeting the exfiltration of defense industry proprietary information could be considered a responsibility of the cyber force or the police, depending on whether it is prioritized as a crime or as an attack against national defense.

306. The information and intelligence secured by a cyber force in the performance of its tasks (monitoring, cyber threat hunting, cyber intelligence) can be useful to national cybersecurity agencies and vice versa. Therefore, the cooperation between cyber force, cybercrime police units, cybersecurity units of other ministries, national intelligence services, national cybersecurity agencies, national critical infrastructure cybersecurity centers and government is necessary to achieve, inter alia, the highest possible level of national cybersecurity.

307. *The industry sector* is one of the main pillars for the development of cyber defense technologies. Therefore, the cyber force must promote cooperation agreements with the industry to foster research, innovation and development of cyber defense technologies.

308. In many cases, acquiring commercial products adapted to the cyber force's operational requirements or the hiring of IT sector private companies for developments or services could be sufficient. But the development, maintenance and survival of the cyber force's

critical capabilities depends on the avoidance of dependence on the private sector, and it is paramount to establish mechanisms that guarantee continued operation of critical capabilities of the cyber force, in the cases in which the corresponding supplier company files for bankruptcy or requires unacceptable conditions.

309. It is necessary to establish specific cooperation environments or agreements with the industry that will allow the cyber force access to the intellectual property and basic knowledge of the products, tools or critical systems acquired, so that, in case of the disappearance or a soured relationship with the provider company the cyber force can continue its operations.

310. *Academia* is another of the pillars for the development of cyber defense technologies, hence, the cyber force must promote cooperation agreements with universities, research and development centers, foundations and think-tanks that promote innovation and development of cyber defense technologies.

311. *Internal cooperation* is the collaboration founded between all the cyber force units; and between command, operational and technical capabilities. All cyber force units must cooperate with each other to achieve the strategic objectives that the commander has identified in the development plan. This is the most necessary cooperation, alas, it is frequently the most forgotten.

312. Internal cooperation is complicated due to the need to reconcile information exchange between units and confidentiality of many activities. Cooperation and confidentiality are two fundamental aspects that must be considered together, designing mechanisms that promote information exchange within secure environments. One thing to avoid, by all means, is for confidentiality to be used as an excuse to create watertight compartments that deny flow of information between the parties in need.

Representation

313. There are *numerous national and international forums,* where important and interesting cyber defense issues are discussed and decided. The cyber force must identify the most relevant, and actively participate in them to learn first-hand about the national or international situation of cyber defense and to influence decision-making to serve, as far as possible, its strategic objectives.

314. The cyber force must assert its role as the *primary head of national cyber defense* to represent the country in cyber defense matters in international and national forums, ahead of other parties involved (national security agencies, intelligence services, law enforcement, etc.) with less responsibility for national cyber defense. The difference between national cybersecurity and national cyber defense have to be explicitly stated in all related national level documents, such as the national defense policy or the national cybersecurity strategy.

Knowledge management

315. *Knowledge management (KM)* is one of the main capabilities for the cyber force operation; its purpose is the distribution of knowledge among the stakeholders and facilitating its access according to the criteria of need and authorization.

316. Knowledge management is a capability that is based on two areas: functional and technical. The functional area is the fundamental and most complex because it requires a personalized approach, and procedures adapted to the unit's particularities and needs; while the technical area can be solved with widespread commercial tools and procedures.

317. *The KM functional area* focuses on the needs assessment for exchange and access to information by all the cyber force units, the design of the information flow map, the development of procedures and rules for access to information, the evaluation of the effectiveness of procedures and tools, and the monitoring of compliance with standards.

318. *The KM technical area* focuses on identifying, testing, implementing, administering and sustaining the appropriate information management and information exchange tools for the effective performance of all the cyber force tasks and activities. Typically, this area is buttressed by the cyber force technical support branch.

319. Knowledge management is a discipline of such influence on the cyber force operation and of such complexity that it is necessary to establish a specific responsible branch, with special qualifications, and exclusive dedication, within general staff (thus highlighting its functional nature over the technical).

320. Knowledge management comprises four main groups of activities: internal information management, management of information exchange with external entities, preparation and updating of a catalog of experts, and preparation and updating of a critical service catalog.

321. *Internal information management* includes the design, development, implementation, administration and maintenance of the cyber situational awareness (CSA), internal databases, think-tanks and platforms for the exchange of information, vulnerabilities and threats (MISP); differentiating classified, unclassified and public information.

322. *External information management* includes the information exchange with the cyber force partners (other armed forces units, other MoD branches, public entities, industry, academia, citizens, cybers forces of other nations, international military alliances, international cybersecurity organizations, etc.) and the management of the public communication strategy.

323. *The cataloging of experts* is an activity aimed at the identification and classification of people and companies especially qualified in an area of knowledge or technologies of special interest and criticality for the cyber force. The catalog of experts must be updated periodically and it must include emerging areas of knowledge and technologies, new experts and new contact details. This activity is closely associated with cyber reserve management.

324. *The cataloging of critical services* is an activity aimed at identifying and classifying critical information systems and services for the operation of the cyber force in accordance with the criteria established by the commander for this purpose. This activity is closely associated with the management of the operations continuity plan.

325. Knowledge management is an essential capability of the cyberspace force, but due attention is often not paid to it. Therefore, it is very important that the cyber force commander explicitly highlight its importance and need (the functional area in particular) and establish the mechanisms and resources necessary for its design, development, implementation and sustainability in the cyber force development plan.

Analysis and lessons learned

326. *The analysis and lessons learned* capability is based on the implementation of a systematic process in order to consider, document, analyze and value the experiences gained in past projects, activities and situations that must be actively taken into account in similar future projects, activities and situations by the same or new actors.

327. This capability, often neglected, is critical for the cyber force given the budding maturity level of the cyberspace domain of operations. The lack of experience and knowledge will prompt the cyber force, not infrequently, to make baseless decisions, which could lead to erroneous, inappropriate or ineffective results. These should be avoided or modified in similar future situations, or contrariwise, in optimal results that must be included in similar future situations.

328. This capability must be especially supported by the knowledge management capability; it must feed the processes of formulation of the cyber defense doctrine and it must serve the cyber force commander in assessing the effectiveness of the organization, means and procedures implemented and alignment with the objectives stated in the development plan.

Financial service

329. *Ordinary financial resources* are needed by the cyber force to ensure the acquisition, sustainability and evolution of the planned capabilities.

330. The dynamic nature of cyberspace requires the establishment of agile hiring mechanisms and flexible financial planning; otherwise there is a risk of collapsing the procurement processes of the new capabilities.

331. In addition, the cyber force needs *atypical financial resources* for urgent acquisitions and the purchasing of highly confidential products and services or products that are not available in ordinary markets.

Legal service

332. The cyber force needs its own legal service with full dedication to cyber force/cyber defense matters.

333. The cyber force legal service should be made up of jurists specialized in computer law and, in particular, in the application of international law to cyber operations both in wartime and in peacetime.

334. The main task of the cyber force legal service is advising the commander on ordinary and operational legal matters and the pursuit of justice in the field of cyber force/cyber defense.

335. *Ordinary legal issues* are related to the ordinary life of the cyber force such as contracts, collaboration agreements, technical agreements, non-disclosure agreements (NDA), legal matters related to personnel and discrimination, etc.

336. *Operational legal issues* are related to the enforcement of national and international law in cyber conflicts, area of operations and exercises, and in particular the application of jus in bello (acceptable practices during war) and jus ad bellum (legitimate reasons to go to war) in cyberspace. The legal service, in addition, must have a relevant active participation in the drawing up of the rules of engagement in cyberspace (cyber-specific ROEs).

Operational capabilities

337. The cyberspace force must have capabilities aimed at conducting cyber operations (defensive, exploitative, and offensive), such as security and information event management (SIEM), operational intelligence, response, digital forensics and deployable cyber defense.

Security event management

338. Currently, there is an unclear use of several terms (NOC, SOC, CERT, CSIRT, CyOC) to designate organizations with cybersecurity responsibilities, creating confounding situations and contradictory perceptions that hinder understanding and collaboration when facing cyber threats.

339. *Network Operations Center (NOC)* is an operational center that monitors its own network and systems in order to preserve the operation and availability of services. It must have the capability to detect malfunctions and interruptions of services. The reaction capability is limited to failure prevention and service recovery within its own network.

340. *Security Operations Center (SOC)* is an operational center that monitors its own networks and systems in order to preserve their security. It must have capability to detect malicious activities targeting its own networks and information. Its reaction capability is limited to preventing, detecting and stopping malicious activities within its own network.

341. *CERT*[25] is a registered trademark owned by Carnegie Mellon University that refers to an entity, normally associated with a specific sector (government, defense, university, banking, business, critical infrastructure, etc.) created with the purpose of preventing, minimizing or eliminating computer security events or incidents. The use of the term CERT requires the express permission of Carnegie Mellon University.

342. *CSIRT*[26] is a generic term for a team with a purpose similar to CERT, but with unrestricted use and therefore requires no authorization.

343. The terms CERT and CSIRT are commonly used to grant a SOC with an official character, recognized and registered by international organizations (FIRST[27], TF-CSIRT[28], EGC Group[29]) that coordinate all associated CERT/CSIRTs and facilitate information exchange on vulnerabilities, threats and mitigation measures.

344. A Cyber Operations Center (CyOC) is a coordination center for military operations in cyberspace, including defensive, exploitative and offensive operations, inside and outside its own network, according to the legal principles of use of force.

345. The cyber force, as the main entity responsible for national cyber defense, must have a cyber operations center (CyOC) that coordinates the action of all SOCs established within its scope.

346. It is very important to clearly define and detail the responsibilities and tasks of the CyOC and subordinated SOCs and NOCs to create trusted collaboration environments to manage tasks with shared, overlapped, uncertain or controversial responsibility.

347. Each type of center (CyOC, SOC, NOC) is made up of personnel with different professional qualifications, operating with different tools and having a different purpose and scope. A SOC basically requires traditional security information and event management (SIEM);

a CyOC requires security orchestration services (SOAR), cyber threat hunting, advanced deception platforms and command and control systems; while a NOC requires tools to control and monitor network operation.

348. Security event management can be grouped into three echelons: the first echelon comprising prevention activities against failures and cyber attacks; the second echelon comprising standard ongoing cyber attack mitigation activities (real-time monitoring, event correlation, indicators of compromise, cyber situational awareness, dynamic risk management, early warning and help desk); the third echelon comprises ex-post analysis and advanced threat mitigation activities (forensic analysis, rapid reaction teams, malware analysis and APT early warning).

Operational intelligence

349. *Cyberspace-related intelligence* can be understood in two ways: cyber threat intelligence, essential to the cyber force; and cyber-supported intelligence services that the cyber force can provide due to its special skills.

350. *Cyber threat intelligence* is the activity performed, mostly through cyberspace and occasionally through other means, to obtain information and knowledge of known or unknown cyber threats, current or potential.

351. Cyber threat intelligence is used to predict future situations; evaluate and assess its own and adversary vulnerabilities; evaluate and assess the cyber defense capability of adversaries; locate targets; prepare its own cyber attacks and anticipate cyber attacks from adversaries; identify its own and adversary critical services; conduct cyber espionage and information exfiltration operations; and create influence.

352. *Cyber-supported intelligence* is the activity carried out through cyberspace to obtain information and knowledge of any matter and that the cyberspace force, as a specialized force in the use of cyberspace, can carry out in support of intelligence services or any other unit that requires it, usually through a request for information (RFI).

353. The cyber force must actively participate in national and international forums that aim to exchange information on vulnerabilities and threats and must foster bilateral agreements with other foreign cyber forces to supplement its internal cyber threat intelligence production.

Response

354. *Response* is the cyber force capability related to offensive cyber operations.

355. *Offensive cyber operations* on alien networks without authorization are very complex operations that require highly sophisticated skills and knowledge and will only be conducted on extraordinary occasions when the use of force is legally permitted. For this reason, the cyber force response unit will dedicate most of its time to its own training, to carry out practices in isolated environments (cyber range) and to participate in cyber exercises in order to be prepared to act when necessary.

356. The *complexity* of offensive cyber operations lies in the difficulty in creating the desired effects while avoiding any trace (fingerprint) to evade detection, prevent technical and legal attribution and prevent the reuse of the cyber weapon by the adversary.

357. In practice, collaboration with other foreign cyber forces, in terms of offensive cyber operations, is very difficult to achieve; so, in this matter the cyberspace force must seek self-sufficiency through its own developments and confidential collaboration agreements with the industry and universities.

358. In international collective defense organizations, such as NATO, the organization itself lacks combat forces (except in very specific cases), so it creates forces for specific missions and operations with the voluntary contribution of nations (force generation).

359. In a cyber defense context, it is mostly unnecessary to deploy cyber defense units to create the desired effects indicated by the mission commander, so the generation of a cyber force is not an efficient mechanism. In this case, an effects generation model is more suitable because a mechanism is established to create a collective cyber effect capability, for specific missions and operations, with the voluntary contribution of nations.

360. For the response, in addition to the regular permanent facilities of the cyber force, other non-regular facilities that cannot be associated with State entities should be considered.

Digital forensics

361. No matter how solid the network defense is, it is not possible to repel all cyber attacks. Consequently, it is necessary to have a service with the capability to study the nature of the cyber attacks in detail once they have occurred, analyzing the malware and the TTPs used and identifying the origin.

362. *Digital forensics* uses special techniques that allow extracting encrypted, damaged and apparently deleted information, preserving the original information, as far as possible. The cyber force must consider two different digital forensics services, the regular and the battlefield services.

363. *Regular digital forensics* is the permanent service of the cyber force, made up of experts specialized in techniques and digital forensic science, aimed at obtaining detailed information on cyber attacks on its own networks.

364. A regular digital forensics team normally performs its work in optimal conditions of time, place and resources and therefore must strive to use forensic techniques and procedures very carefully and cautiously, to extract all possible information without damaging the original source, so that it can be used as evidence in court proceedings.

365. *Battlefield digital forensics* is a specific mission-oriented service for the extraction of information in the networks of adversaries. It is normally provided in three echelons: the first echelon is the information extraction team; the second echelon is the battlefield forensics team; and the third echelon is the regular forensics service.

366. *The information extraction team* is made up of personnel from forces not specialized in forensic techniques (usually special operations forces) who, with basic forensic training and in the shortest possible time, must extract information and information devices from adversary networks, in hostile territory, in the best possible way so that this information can be analyzed by the battlefield forensic team or by the regular cyber force forensic service.

367. *The battlefield forensic team* is a deployed expert team that performs a quick analysis of the information extracted by the extraction team, in order to obtain useful information for ongoing operations.

368. *The regular forensics service* is responsible for carrying out a more detailed analysis with the available information, in order to obtain useful intelligence for future operations.

369. In the context of a military campaign, the extraction team will strive to obtain information and devices, in the best and quickest way possible, so that it is useful for the second echelon without considering the potential damage to the original information that could affect a subsequent court proceeding. In this case, speed and information about the adversary take precedence over legal evidence preservation.

370. One of the problems that the regular digital forensic investigation service usually encounters is malware *obfuscation*[30] to hinder software reverse engineering[31] and detection by antivirus or human analysts.

371. Digital forensics should be closely associated with cyber threat hunting.

Deployable cyber defense

372. In some cases, when technical, operational or procedural issues do not allow cyber defense actions to be carried out remotely from the main cyber force facilities, part of the capabilities must be deployed to tackle specific defense, exploitation or attack situations.

373. The cyber force must have *deployable cyber defense teams* made up of personnel, means and procedures that are customizable (according to the mission) and transportable (by regular military or civilian means of transport), trained and prepared to deploy wherever required (areas of operations, exercises, facilities or platforms in other domain of operations, critical infrastructure facilities, etc.), in the shortest possible time, in order to reinforce existing cyber defense or handle urgent critical situations.

374. Deployable cyber defense teams must be able to be configured hastily, in a specific *mode of operation,* both in tools and personnel, according to the mission. The most common specific modes of operation are defensive (monitoring and security event management, audit, digital forensics and APT protection), while the exploitative and offensive modes could be provided occasionally.

Technical capabilities

375. The cyber force must have capabilities to provide technical support to the command and operational capabilities, such as IT security audits, cyber range, technology observatory, research and development, arsenal, information security, and cryptography.

IT security audit

376. Regarding information technology systems (IT systems) three main authorities must be differentiated: the owner or operational authority, the administrator or technical authority and the person responsible for security or security authority.

377. *The IT system operational authority* is the highest rank of the units, functions or services that the system serves, those that use the system, and which are affected by a failure or interruption of it when performing their tasks. The system operational authority is responsible for defining operational requirements and designating and authorizing users.

378. *The IT system technical authority* is the highest rank of the communication and information systems (CIS) units in charge of the design, development, administration and sustainability of the system according to the operational requirements established by the operational authority and the security requirements established by the security authority.

379. *The IT system security authority* is the highest rank of the cyber defense units and is in charge of defining system security requirements and monitoring compliance with security norms.

380. The establishment of the three authorities (operational, technical and security) provides balance and stability to the systems and, therefore, their responsibilities should not be transferred or delegated between them.

381. *The IT system security audit* is a mechanism that the operational authority has available to reliably know the security level of the IT systems under its responsibility.

382. In an IT system security audit, the auditee is the CIS unit (subordinate to the technical authority) administering the system to be audited and in accordance with the principle of auditor independence (auditee and auditor cannot fall under same authority). Therefore, the auditor should be a unit that is subordinate to the operating authority or the security authority, where the latter is the most recommended considering that it has the appropriate staff, means and knowledge.

383. IT security audits have to consider all aspects (technical, physical, human and procedural) that affect, in any way, the security of the systems that process classified or unclassified information.

384. IT security audits must analyze and assess the level of compliance or alignment of the software, hardware, facilities, documentation and personnel with the security measures established in the corresponding reference standards.

385. The usual process in an IT system audit is as follows:

1. The audit team (usually a unit subordinate to the security authority) plans and proposes a schedule to the audited unit (CIS unit subordinate to the technical authority) and the operational authority (system owner).
2. The audit team studies, tests and evaluates the proper controls, according to the information provided by the audited unit.
3. The audit team performs the audit.
4. The audit team prepares the audit report and distributes it to the audited unit so that the deficiencies can be corrected within a defined period.
5. The audit team scales the report to the security authority, which, in turn, submits it to the operational authority.

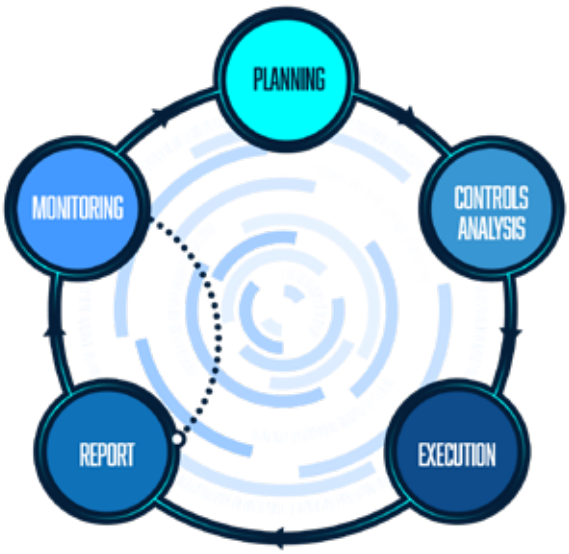


FIGURE 26. IT SYSTEM SECURITY AUDIT CYCLE

386. Typically, in the case of *classified systems,* they need to be previously accredited by the operational authority before they are allowed to start operating or be reaccredited so that they can continue to operate. In this case, the audit report would contain not only the results of the audit, but a positive proposal (i.e., the system is free of serious deficiencies that prevent it from operating) or a negative proposal (i.e., the system has serious deficiencies that prevent it from operating).

387. *Accreditation* is usually granted for three-year periods, but, as technology and system classification allow, ideally, dynamic online audits that are capable of evaluating systems in real time should be performed.

Cyber range

388. *Traditional military range* is a restricted area of a land, sea or air domain that is used to train military units and carry out live-fire exercises in a safe and isolated environment that ensures doing no harm to the area involved.

389. In order to be more effective, the military range should be designed to resemble the most probable terrain where the operation to be trained or tested would take place. An opposing force should be included.

390. *Cyber range* is exactly the same as a military range; that is, it is a restricted area of cyberspace that is used to train cyber defense units and practice live-fire cyber exercises in a safe and isolated environment that ensures doing no harm to the cyberspace area involved.

391. The cyber range is actually more effective than traditional ones, since it can simulate, quite accurately, the environment where cyber operation would take place, including topology and network activity, user behaviors, and a live-fire enemy.

392. The cyber force needs the cyber range to conduct, among other activities, individual and collective training; model and simulate environments, scenarios, networks, effects and behaviors; analyze malware; develop cyber weapons; and test, evaluate and validate concepts, products, technologies and TTPs.

393. The cyber range of the cyber force must be secure (it must allow selective access exclusively to authorized users), isolated (it must prevent the effects of the activities carried out on it from spreading outside of it), reliable (it must reproduce the activities as required by users), accessible (on-site and online), scalable (it must easily allow for increased capability and power), dynamic (it must evolve as new technologies emerge), comprehensive (it must be able to simulate any IT environment required, including industrial control systems), resilient (it must be robust to failures, including a backup cyber range) and most importantly, it must be operated by a multidisciplinary team, expert in virtualization technologies and modeling and simulation tools, and very knowledgeable of the cyber defense technical and operational environment.

394. The ideal case for national cyber defense is the development and implementation of a *national cyber range* in which the Internet can be modeled to carry out response practices to large-scale cyber incidents, with the participation of the cyber force and other actors, public or private, involved in national cyber defense.

Technology observatory

395. The global market offers innumerable technologies, products, tools and companies of interest and useful for current and future cyber defense.

396. The vast majority of cyber force personnel do not have time to examine and test the technologies, products or tools of potential interest to their field of activity, or to attend the myriad events that are continuously organized, or to hear companies that promise ideal and innovative solutions. Therefore, it is necessary to establish a cyber force branch (technological observatory) that is dedicated exclusively to technology observation and, in this way, free the rest of the staff from an avoidable work overload.

397. The responsibilities of the technology observatory are: to analyze and test the technologies, products and tools on the market, and assess their maturity and potential usefulness for the cyber force; receive companies in the sector and assess the potential usefulness of the solutions they propose; attend the most relevant events related to cyber defense and assess and report on products and trends; inform potential beneficiaries of the results of their findings and evaluations; prepare a catalog (normally on an annual basis) classifying all the technologies, products and tools considered potentially useful for the cyber force and national cyber defense; and identify and report on sources for obtaining exploits and zero-day vulnerabilities.

Research and development

398. In order to keep an acceptable competitiveness level in the global cyber defense environment where the cyber force operates, it is necessary to have a permanent and stable research and development capability.

399. The research and development of new cyber defense technologies and the adaptation of technologies from other sectors for use in cyber defense is such a formidable task that the cyber force cannot perform it alone. It must manage it jointly with the MoD R&D branch and in collaboration with public R&D centers, industry and academia.

400. The study of the application of emerging technologies (artificial intelligence, machine learning[32] , blockchain[33] , big data[34] , 5G[35]) to cyber defense or the use of novel means such as RPAS[36] is also necessary to keep an operational level equivalent to other cyberspace forces in the same geostrategic environment.

401. *Research* is a necessity to improve future cyber defense, but many of the results are not immediately applicable in the cyber force. With proper programming, the results could be applicable in the medium or long term. Therefore, it is very important to keep multiannual programs and to manage, control and evaluate the results in the medium and long term.

402. The implementation of the research results is very diverse, and it may serve to create new tools or products, to improve existing technologies, to support new developments, to promote or improve existing developments or to rule out other less efficient research areas or which are not appropriate to cyber defense needs.

403. The cyberspace force usually needs to carry out three types of development (self-development, external and cooperative) to maintain its operational level

404. *Self-development* is conducted by the cyber force with its own human, material, cognitive

and financial resources. It may include acquiring commercial products to solve specific parts of the development package, but the management, design, integration of all parts, implementation, evaluation and validation is always carried out by the cyber force. In a self-development project, only the cyber force has the complete knowledge of the development and its functionalities.

405. Self-development may be necessary, inter alia, due to shortage (there is no external support), financial incapacity (there is no external financial prospect), security (information on the product, its development process and functionality are highly classified, so confidentiality would be jeopardized by collaboration with third parties), time restrictions (public procurement and development processes may be too slow to respond to urgent needs), profitability (it is a less expensive option) and suitability (the cyber force has the best skills).

406. *External development* is carried out by an external entity, in accordance with the operational and, sometimes technical, requirements established by the cyber force through a contract.

407. *Cooperative development* is carried out jointly by the cyberspace force and other entities through a cooperation agreement.

408. Typically, the cyber force will need to carry out the three types of development: self-development for sensitive or urgent needs; external for the long-term; and cooperative for complex developments.

Cyber arsenal

409. The cyberspace force, like any military unit, needs weapons specially designed to cause specific effects in cyberspace, the consequences of which may transcend to the other domains.

410. In order to have adequate armed capability to carry out its missions, the cyber force must establish mechanisms and procedures to acquire and develop cyber weapons and payloads to configure the cyber arsenal.

411. Cyber weapons and payloads can be acquired on the global market, regular or irregular, through the national arms industry, or through self-development or cooperative development.

412. National cyber defense needs a robust *national cyber arms industry* to avoid external dependency that may jeopardize current and future operations, as occurs with traditional domains.

413. The cyber force needs to acquire cyber weapons on a regular basis and, furthermore, develop its own cyber weapons (new weapons, customizing known weapons or reusing captured weapons from cyber attacks it has sustained) and testing them in the cyber range.

414. Cyber arsenal configuration is one of the cyber force's most sensitive tasks and it must be done in such a way that ensures that the cyber arsenal is secure (it must allow access only to authorized personnel), reliable (cyber weapons must be tested and frequently updated, guaranteeing that they perform as expected), recordable (it must record cyberweapon usage to avoid repetition in same objectives), scalable (it must easily allow increase) and complete (it must include all the cyber weapons required for the cyber attacks in the cyber force operations and missions).

415. Compared to traditional domains, the cyber force arsenal is more dynamic, continually incorporating new cyber weapons and redesigning old ones, so that cyber weapons used in a cyber attack cannot be detected through recognized fingerprints, and if they are detected, that they not be reused by the victim. For this reason, in many cases, they are single-use cyber weapons and are designed to self-destroy under certain conditions.

Information assurance and cryptography

416. *Information assurance* is a basic service in the cyber force, given the sensitive nature of most of its operational, technical, hiring and procedural activities.

417. Information assurance is a cross-domain service, for all domain of operations, aimed at preserving the availability, integrity and confidentiality of information. It is one of the many services that the cyberspace force needs, and it must not, under any circumstances, be mistaken or assimilated to cyber defense.

418. Information assurance must consider all the components that interact with information, in one way or another, such as people, documents, facilities, IT systems and companies.

419. The cyber force information assurance branch is responsible for developing information assurance rules and procedures and for monitoring and promoting compliance with them.

420. *Cryptography* is a matter that is ubiquitous in most cybersecurity services and measures, being fundamental not only in the obvious confidentiality aspects but also in many other sensitive services such as access control, digital signature, integrity, etc. Many cyber attacks include cryptography in some phases, therefore, it is critical for the cyber force to have an adequate cryptography branch to handle cryptographic matters related to cyber defense.

Facilities

421. *Facilities* of all cyber force units must be adequately equipped to accommodate the matériel and personnel in the proper safety, operational and environmental conditions.

422. Cyber operations, to a large extent, take place in confidential environments; therefore, the facilities must be conditioned to protect the confidentiality of information and activities to their required level.

423. In addition to regular facilities, the cyber force must consider the permanent or temporary use of *covert facilities* necessary to protect the anonymity of sensitive cyber operations and to disassociate them from State entities or national territory.

Command

424. Cyber defense is not a joint function, but a combat capability specialized in the cyberspace domain of operations. Hence, it must be subordinated to an *independent command* from the other domains, even when the size of the cyber force is small.

425. The complexity of the organization and the coordination of cyber defense, as well as its ability to create immediate strategic effects, requires having a *single command* that depends on the highest operational levels: the joint force commander, the chief of defense and the minister, each in the individual's scope of action.

Cyber threat

426. *Cyber threat* is an external or internal potential source of damage to an organizational asset, which materializes through cyberspace. It exploits a technical or human cyberspace vulnerability, affecting valuable assets for the organization or for the cyber threat source itself.

FIGURE 27. CYBER THREAT

427. A source is considered a cyber threat if it meets three requirements: capability, interest and hostility.

428. The cyber threat must have the *capability* to identify and take advantage of the vulnerabilities of the victim's networks and IT systems and to cause harmful effects.

429. Capability can be configured on its own technical and human capability or surreptitiously compromising third parties' technical capabilities (botnets), hiring or subcontracting someone else's capability (universities, commercial companies or criminal groups) or influencing actions on people to generate the desired malicious actions (taking advantage of unstable or conflicting social, economic or political situations).

430. The cyber threat capability must be considered in relation to the potential objectives, since, for instance, the capability necessary to create a STUXNET-type cyberattack is not the same as a ransomware[37] or a website defacement[38].

431. The cyber threat must have an *interest* in the victim's assets. In other words, the assets of the potential victim, especially information, must have a profitable value for the threat source, in such a way that the expected benefits offset the cost of the resources necessary to carry out the cyber attack.

432. Finally, the cyber threat must have hostility toward the potential victim, that is, an interest in causing harm to its IT networks and systems, even if it does not provide a direct benefit, but an operational advantage in the context of a conflict or a competition.

433. *Identifying cyber threats* is a three-phase process. First, the sources (States, organizations, individuals or entities) that have an interest in the potential victim's assets are listed; second, among the sources in that list, those with the capability are singled out; and third, the sources that, even having an interest and the ability, are be ruled out because they have an alliance with the potential victim.

434. In some cases, belonging to the same political, economic or defense *alliance* is not enough to rule out the source as a potential cyber threat, since, if the interest is big enough, they could try anonymous cyberattacks (taking extreme care to avoid actions that may be tracked) or conduct false flag cyberattacks.

435. Cyber threats to national and military interests are increasingly common, sophisticated and damaging. For this reason, cyber defense must be incorporated into military planning at all levels of command and cyber threats and cyber risks must be taken into account throughout the entire cycle of joint operations planning.

436. There are basically two types of cyber threat sources: internal and external.

437. *Internal cyber threat sources* are the individuals or entities that belong to the organization of the potential victim and, therefore, are authorized to access the data, information or systems of the targets; or the individuals or entities acting from within the organization because, although not belonging to it, they have maliciously obtained access credentials. The causes of internal cyber threat are usually due to ignorance, accidents, negligence or deliberate acts.

438. To prevent internal cyber threats due to *ignorance*, it is necessary to conduct cybersecurity training and awareness at all levels of the organization; as well as monitoring compliance with cybersecurity standards, measures and procedures and assessing effectiveness.

439. To prevent internal cyber threats due to accidents, it is necessary to develop operation continuity plans and implement a transparent cybersecurity model to minimize having end users make cybersecurity decisions.

440. To prevent internal cyber threats due to *negligence*, it is necessary to use basic internal monitoring (based on SIEM) and to establish a simple cybersecurity model where the security measures to be applied by end users are easy to understand and put into practice.

441. To prevent internal cyber threats due to *deliberate acts,* it is necessary to establish advanced monitoring models based on cyber threat hunting (para. 478) and to carry out internal IT security audits.

442. *External cyber threat sources* are the individuals or entities that do not belong to the organization of the potential victim and, therefore, are not authorized to access the data, information or systems of the targets. In a practical way, they are grouped into three types: States, organized groups and individuals.

443. To combat *State cyber threat* requires the involvement of a cyber force and participation in collective defense alliances in international organizations such as NATO or IADB and multinational and bilateral cyber defense agreements.

444. To combat cyber threat from sources not attributable to States (i.e., organized groups or individuals) it is necessary to strengthen the three pillars of national cybersecurity (cyber resilience, cyber protection and cyber defense, para. 530), have close cooperation between them and apply the related international law.

445. The most common targets of cyber threats are information, IT networks and systems, mobile communication devices (smartphones, tablets) and critical infrastructure control and information systems. Nonetheless, indirect physical consequences to facilities and people cannot be ruled out.

446. The cyber threat to *mobile communication devices* (smartphones and tablets) must be considered distinctly because these devices have additional cyber risks.

447. Despite the fact that a current mobile device is a computer system in itself, the need to protect it against cyber attacks is not perceived to the same extent as conventional IT systems (computers, computer networks, etc.). This lack of awareness makes these devices especially vulnerable.

448. Mobile devices are exceptionally attractive for cyber threats, because they are multi-format (data, voice and video) and multipurpose (ByOD[39]); they are an extension of the owner with a camera and a microphone. Except in cases of specific restrictions, they are usually with the owner at all times, attending meetings and discussions, and seeing and hearing the same that the attendees are doing. They are also potentially geolocatable.

449. *Cyberattacks on mobile devices* in order to control applications, camera and microphone are not difficult for expert cyber attackers, even when the device is turned off.

450. Other targets to pay special attention to are *critical infrastructures* because an impact on them could have devastating consequences at the national level.

451. The globally accepted critical infrastructure sectors are energy, public health, water supply, agriculture and food, banking and finance, information technologies, transportation, chemical industry, nuclear industry, space, research and development, and public administration.

FIGURE 28. CRITICAL INFRASTRUCTURE SECTORS

452. There is a false perception that critical infrastructures do not connect to the Internet and therefore are not at risk of a cyber attack. Not only do most of the information systems that control critical infrastructure connect to the Internet, but those few that are isolated are also vulnerable to cyberattacks.

453. All the strategic sectors have many facilities located in different geographical locations, a long way from each other. Therefore, decentralized management and maintenance would mean an unaffordable multiplication of resources for critical infrastructure operators, most of which are private companies oriented towards economic benefits. For this reason, all the systems that control critical infrastructures, to a greater or lesser extent, are connected to the Internet to have a centralized management and maintenance system.

454. The criticality of the critical infrastructure sectors together with its global connectivity requires extreme protection against cyber threats for the critical infrastructures and, in particular, the electricity and IT sectors, since the rest of the sectors depend on them to operate.

Cyber threat landscape and trends

455. Every year, studies and reports are published, analyzing the *cyber threat global landscape and trends* (CCN/CERT[40] , ENISA[41] , Gartner[42] , CheckPoint[43] , FireEye[44] , Kaspersky[45] , among many others). These studies mix cyber threat sources (States, terrorists, hacktivists, etc.) with cyber attack types (phishing, DNS attack, etc.) and targets (mobile devices, supply chain, fake information, credentials theft, etc.) and the information is examined from different points of view.

456. According to the 2019 "cyber threats and trends" report of the Spanish national CERT (CCN-CERT), the most significant cyber threats on the international context are the States and the groups sponsored by them. Other relevant cyber threats are attacks on the supply chain, actions in cyberspace by terrorist groups, jihadists and hacktivists, fake news, as well as attacks on personal data (with the ultimate aim of committing certain crimes, stealing credentials, phishing or espionage).

457. The Check Point report (Cyber attack Trends: 2019 Mid-Year Report) reflects a different picture, with another point of view, emphasizing the increase of four types of attacks compared to the previous year (software supply chain attacks on the rise, email scams gearing up, attacks against cloud environments, and evolving mobile landscape) and the persistence of three other types of attacks (ransomware, cryptomining[46] and DNS attacks[47]).

458. All reports are useful but need to be analyzed in a proper perspective. Consequently, it is recommended that each pillar of national cybersecurity (cyber force, police and CSIRTS) prepare its own report on cyber threat landscape and trends based on its own intelligence, potential objectives and analysis of reports from reputable sources of diverse origin and geostrategic positioning.

459. In any case, it can be confirmed that, currently, the *State cyber threat,* through special offensive cyber defense units (APTs), is the main threat to contemplate at the national level, as has been publicly recognized by NATO and NATO nations.

Advanced Persistent Threat

460. *Advanced Persistent Threat (APT)* is an organized group of experts, normally associated with a State, who use sophisticated knowledge, tools and TTPs (techniques, tactics and procedures) to infiltrate, take control of and persist in an alien network (anonymously, stealthily and unnoticed) in order to have access to select information and obtain strategic advantages.

461. An APT usually operates according to a 5-phase cyclical process: preparation, access, persistence, execution and anonymization.

462. In the *preparation phase,* the potential objectives are identified and the assets and profitability of the cyberattack are assessed by comparing their own resources required for the development of the cyberattack and the expected benefits.

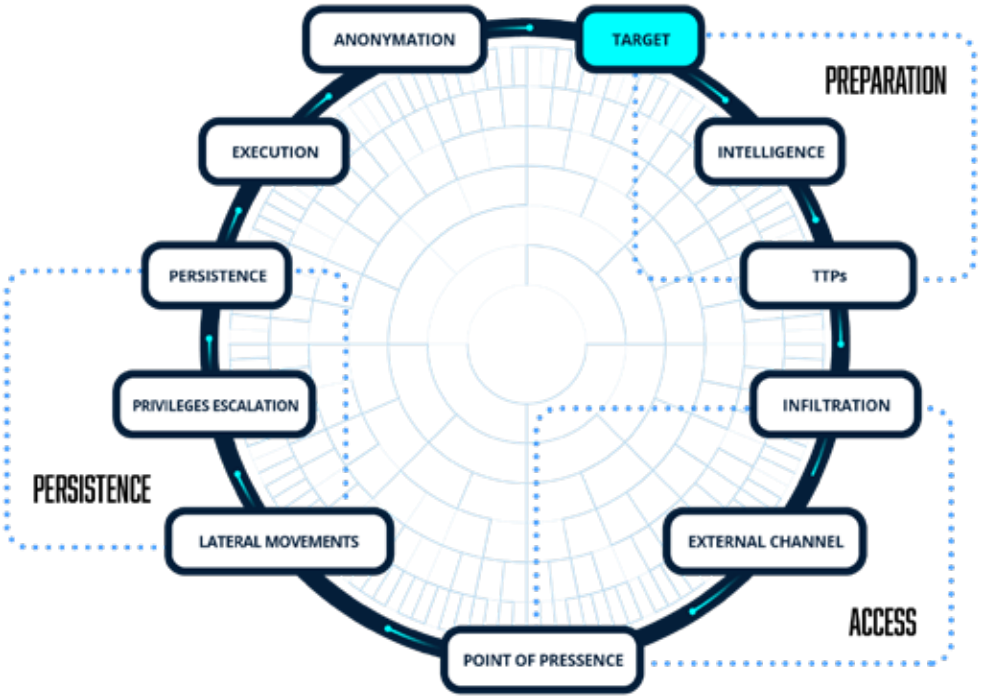


FIGURE 29. APT CYCLE

463. Then, intelligence of the potential victim is gathered, including the organization, cyber defense capability, vulnerabilities, and any information that could be used as an attack vector (emails, websites, etc.) or to support cyber attacks (names, positions, organization, roles, responsibilities, expected behaviors, usual activity on the network, etc.) using both passive and active exploitative cyber operations.

464. Once the target has been selected and with all the available intelligence, the most suitable cyber weapons, payloads and TTPs are selected from the arsenal and the cyber attacks are designed and tested in the cyber range to verify effectiveness and anonymization.

465. In the *access phase,* the APT infiltrates the target network and establishes an external communication channel.

466. The infiltration is carried out taking advantage of previously detected vulnerabilities (usually through spear phishing or watering hole) and once inside, a malware is installed to create a backdoor (hidden remote access) managed by a remote administration tool (RAT).

467. Once the back door is created, a hidden communication channel is implemented between the target network and the APT command and control center, establishing the first point of presence.

468. In the *persistence phase,* the first point of presence is used to conduct a detailed reconnaissance of the network from within, providing the necessary information to carry out secure and stealthy lateral movements (movements within the network) for the purpose of establishing other points of presence and escalate privileges to obtain a greater, lasting degree of control and achieve more complex objectives.

469. The *execution phase* begins when a sufficiently high degree of control and persistence is achieved to ensure the attack on the strategic objectives without being discovered. In this phase, the selection, collection, encryption and exfiltration of information of interest to the APT associated organization is done cautiously.

470. In the *anonymization phase,* as the specific objectives are achieved, the APT proceeds to cover its tracks to eliminate any potential evidence of the activity and TTPs to hinder detection and potential future attribution.

471. A main premise in APT cyber attacks is to keep control of the network without being detected as long as possible, therefore, in all phases, the APT pays maximum attention to implementing measures aimed at covering its tracks and keeping an activity that can be perceived as usual on the network, including long periods of inactivity if necessary.

472. APT cyber attacks are of such magnitude, sophistication and complexity and their objectives are of such criticality that action to combat them must be planned, coordinated and developed on a *specific military cyber operation.*

473. Combating APTs that threaten military objectives requires action led by the cyber force and coordination and collaboration with the network operations center (NOC) and police cybercrime units.

474. Collaboration with the network operations center is necessary because many defensive measures have to be implemented by it and, on some occasions, the measures will affect the operation of the network, including temporary interruptions of critical services.

475. In cases affecting the operation of the network, the operational authority of the affected systems must make decisions considering the arguments of the cyber force (security authority) focused on the eradication of the APT and the arguments of the NOC manager (technical authority) focused on keeping the network operational.

476. Collaboration with police cybercrime units is necessary in the cases that it is considered that the action of the APT may, in addition, constitute a crime and the pertinent court proceedings could be initiated.

477. The great danger of APTs is that they produce silent effects, which do not attract attention and do not affect the operation and functionality of network's services and systems, creating a false perception of security in senior leaders that are not directly involved in cyber defense but are who, ultimately, make the decisions about resources and measures necessary to cope with them.

Cyber threat hunting

478. *Cyber threat hunting* is a dynamic and proactive cyber defense process aimed at the detection and isolation of advanced threats that evade traditional security solutions based on SIEM and cybersecurity perimeter devices (firewalls, IDS, IPS, sandboxing48, etc.).

479. Traditional cyber defense *(cyber threat detection)* is based on its own network monitoring, mainly at the perimeter, in order to detect cyber attacks by recognizing previously known patterns, anomalies and threats (signature).

480. Cyber threat hunting is based on its own network monitoring, at the perimeter and internally, in order to discover new patterns of cyber attack by automatically identifying unusual behaviors (behaviors that do not adjust to the usual activity of the network) of users, processes, and devices.

481. An effective threat hunting system is a creative process (based on hypotheses and assumptions of noncompliance) materialized through a flexible methodology that bases the success on the knowledge, experience and skills of the personnel who operate it (hunters or analysts) rather than in the tools.

482. Once a new pattern is discovered, a reaction (automatic or human) must be triggered to repel the cyber attack and then a new plan must be designed and implemented, in collaboration with traditional security, to reduce the attack surface. Finally, the forensic investigation service can initiate investigations to discover the causes and origin.

483. In any case, a strong cyber defense needs both types of cyber defense approaches (threat detection and threat hunting) since they complement each other.

484. The current international reference for the preparation of cyber threat models and methodologies is the open access *MITRE ATT&CK*®[49] knowledge base that provides information on TTPs (tactics, techniques and procedures) based on real-world observations.

485. The MITRE ATT&CK® reference provides a technical and operational framework for cybersecurity commonly used in both public and private sectors, facilitating public-private understanding and cooperation.

DOCTRINAL PRINCIPLES

486. Cyber defense is a *combat capability* specialized in the cyberspace domain of operations and not a joint function. It is one more option in the hands of the mission commander to create the desired effects on the battlefield or area of operations or to support other traditional forces.

487. To facilitate the organization and use of cyber defense as a military capability and to ensure its smooth integration into joint action with land, sea and air capabilities, cyber defense needs to be governed by the same doctrinal principles or principles of joint operations (based on the traditional principles of war) and adapt them to the particularities of cyberspace.

488. Military operations are based on different means, resources and tactics for each domain, but must be governed by the *same principles* that ensure intellectual agreement and effective joint action.

489. The *doctrinal principles* that guide the action of the military forces in operations are the fundamental principles (will to win, freedom of action and ability to execute) and the operational principles that derive from the fundamental principles (objective, offensive, mass, maneuver, economy of force, unity of command, security, surprise, simplicity, restraint and perseverance).

490. *Will to win* is the firm intention of the commander and the troops to prevail over the adversary and carry out the mission in any situation, however disadvantageous it may be. In cyberspace, will to win takes on special relevance due to the numerous occasions when a defender will find him or herself at a disadvantage due to combat asymmetry or when an attacker will encounter apparently impenetrable defenses.

491. *Freedom of action* is the possibility to decide, prepare and execute plans despite the action of the adversary. This requires a solid understanding of the adversary's cyber defense capabilities and networks and its own cyber defense capabilities. It is acquired when cyber supremacy or cyber superiority is reached and maintained.

492. *Ability to execute* is the faculty to effectively and efficiently determine, adapt and use the cyber defense means according to the mission, establishing the necessary plans for the deployment of cyber operations, executing them according to the plan and modifying them according to the situation if necessary.

493. Given the dynamic nature of cyberspace, the modification of cyber operations plans will occur not occasionally, therefore, it will be necessary to develop mechanisms to facilitate agile changes in the plans, in order to adapt them to the new situation, according to the information obtained from a solid cyber situational awareness (CSA) and predefined indicators.

494. *The objective* advocates military cyber operations aiming at achieving a clearly defined, decisive and achievable objective.

495. Each component in the cyber operation must know, clearly and unambiguously, the objective (system, network, service, user, information, etc.), the required effect (exfiltration, interruption, degradation, destruction, etc.) and the particular conditions of time and security (anonymity, side effects, etc.).

496. The objective must be profitable. Profitability should be valued according to the comparison between the resources used and the benefit for the mission and not based on valuations exclusively within the scope of the cyber force.

497. *The offensive* consists of seizing, retaining and exploiting the initiative and taking advantage of the already achieved decrease in the cyber defense capability of the adversary, nullifying or unbalancing the adversary's possibilities of action or reaction.

498. The offensive is achieved with cyber supremacy or cyber superiority, whether known or unknown by the adversary.

499. *Known cyber supremacy/superiority* is reached when the adversary knows our movements on their networks and despite this, they do not have the ability to stop our freedom of action.

500. Unknown cyber supremacy/superiority is reached when the adversary is unaware of our movements on their networks and because of that they do not take response actions to stop our freedom of action.

501. Offensive cyber operations are intended to undermine the enemy's operational capabilities in cyberspace, and this can be exploited by the cyberspace force or by forces from other domains. A real case of joint exploitation of cyber operations occurred in the 2008 Russia-Georgia conflict in South Ossetia, in which land operations were planned and conducted together with cyber operations.

502. *Mass* is the concentration of the effects produced by the cyber defense capability, at the most advantageous place and time, to create decisive results for the mission.

503. An example of mass is the distributed denial of service (DDoS) attacks that seek to saturate a service by flooding it with massive legitimate access requests. The DDoS attack proceeds from many points simultaneously on a single target making use of compromised network capability (Botnets[50]).

504. *Maneuver* is the faculty of commanders to modify the orders issued and adapt them to variations in the mission and situation. It is essential in cyber defense, due to the need to adapt defensive and response measures to the continuous change in TTPs of cyber attacks and the need to modify the TTPs in offensive actions to become effective in robust defenses.

505. *Economy of force* is the efficient use of the available cyber defense resources by dedicating those that are essential for the fulfillment of the mission. This principle becomes highly relevant in an asymmetric environment where the resources necessary to defend against a cyber attack are usually much more expensive than those necessary to carry out the cyber attack.

506. When cyber defense resources are scarce, cyber defense capabilities could be centralized at the joint level for more efficient use.

507. *Unity of command* is the assignment of a single commander for each mission, operation or objective at all levels of cyber combat.

508. Unity of command is especially relevant in cyber operations involving actors different from the cyber force, in the understanding that all cyber operations within the framework of national cyber defense must be led by the cyber force.

509. *Security* is the ability to protect their own cyberspace against cyberattacks through proper prevention and reaction.

510. *Prevention* requires measures to reject known and unknown cyber attacks or render them unproductive, as well as exploitative capability to provide accurate and timely information on the TTPs of potential adversaries in order to anticipate potential cyber attacks.

511. *Reaction* is based on the resilience to keep operating, in standard or degraded mode, despite the cyber attack action, being able to restore essential functions after suffering the effects of a cyber attack (by establishing an operations continuity plan) and based on an offensive response that may destroy or impair the adversary's cyber defense capabilities.

512. *Surprise* consists of carrying out cyber defense actions (TTPs) in the place, time and form that is unknown or unexpected by the adversary or for which the adversary is not prepared.

513. *Surprise* is an inherent characteristic of cyber threats, so that not only the place and time chosen by cyber attackers are, in many cases, unknown by the defender, but also the nature of the attack itself, the type, form and tactics employed change very quickly.

514. *Ambushes* (honey pots, honey nets, cyber deception platforms or weaponized decoys) and *zero-day cyber attacks* are examples of defensive and offensive cyber tactics based on the surprise principle.

515. *Simplicity* consists of preparing clear and uncomplicated plans and issuing clear, precise and concise orders to avoid misunderstandings and confusion, facilitate understanding of plans and orders and execution as intended.

516. Keeping the principle of simplicity in mind, at all times, is essential in cyber defense due to the complexity of planning and conducting cyber operations and the speed and dynamism of its execution that requires continuous changes of course.

517. *Restraint* refers to limitation of collateral damages and avoidance of unnecessary use of force.

518. The restraint principle acquires special relevance in cyberspace due to the difficulty of controlling the extent of the effects of a cyber attack, the difficulty of attribution, and the possible use of false flag cyber attacks that could cause a reaction on a compromised third party or that has been wrongly accused instead of on the true cyber attacker.

519. *Perseverance* refers to the aptitude to secure the commitment necessary to reach the final strategic situation.

520. Perseverance in cyber defense does not mean continuing an activity permanently, but keeping the conditions to ensure success, which, at times, could combine periods of activity with periods of inactivity. APTs are an example of the use of the principle of perseverance.

521. Perseverance implies unity of command to secure the commitment of all actors involved to strategic objectives.

522. In the cyber defense environment, where full protection is known to be unachievable in advance, persistence against robust defenses is a determining factor to discover vulnerabilities that will come to light sooner or later.

523. All doctrinal principles are a guide for all domain of operations (land, sea, air and cyberspace), but they gain special relevance in the joint domain.

CYBER ECOSYSTEM

524. *Cyber ecosystem* is the system made up of all the components that are related to each other through cyberspace, together with cyberspace itself. As such, the cyber ecosystem generates its own specific norms and behaviors that enable the development and evolution (individually and collectively) of its components (inhabitants).

525. The cyber ecosystem is composed of three parts: the *components* (inhabitants) that interact with each other (IT infrastructure, software, information, protocols, electrical energy and people), cyberspace itself (habitat) and the *relationships and activities* that take place in or through it.

526. The main characteristic of the cyber ecosystem is the *interaction* between people, individually or in organized groups (companies, public administration, universities, international organizations, etc.) generating all kinds of activities, economic, social, artistic, informative, training, collaborative and also defensive, in all its extension.

527. *Cyber defense* is not just one more activity that takes place in the cyber ecosystem, but it is the activity that allows, within its scope, the free and legitimate exercise of all activities.

528. In this sense, *military cyber defense* is understood as the capability aimed at defending the free and legitimate exercise of all the activities of the Ministry of Defense in cyberspace and, in addition, it is the main capability of national cyber defense and one of the pillars of national cybersecurity.

529. Relevant aspects of the cyber ecosystem related to cyber defense are national cyber security, international cyber security, public-private partnership, third-party risks, cyber risks associated with pandemic situations and information.

National cybersecurity

530. *National cybersecurity* is the part of national security focused on protecting national interests in cyberspace. It is based on three pillars: *National Cyber Resilience, National Cyber Protection and National Cyber Defense.*

531. *National cyber resilience* is the set of national cybersecurity capabilities centered on the prevention and protection of the nation's IT networks and systems against cyber attacks, maintaining operations during their course and restoring essential functions after suffering their effects.

532. National cyber resilience is managed on the national CERTs; mainly government, military, critical infrastructure, universities and private sector CERTs.

533. *National cyber protection* is the set of national cyber security capabilities dedicated to protection against cybercrime and cyberterrorism. It is carried out by specialized units of the police bodies.

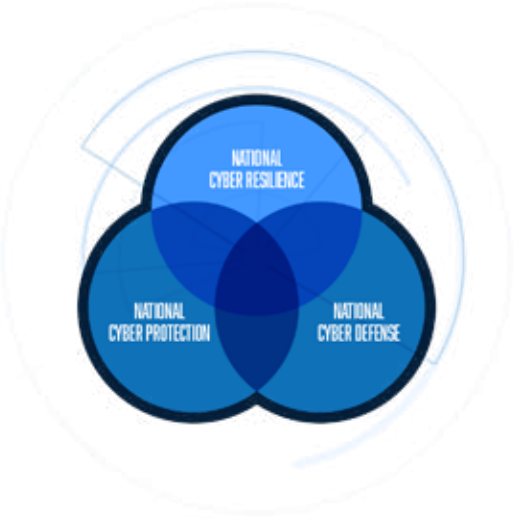


FIGURE 30. NATIONAL CYBER SECURITY

534. *National cyber defense* is the set of national cyber security capabilities (defensive, exploitative and offensive) addressing the defense of national interests against cyber threats from other States or other large-scale cyber threats that could affect national defense. Mainly, it is carried out by cyber defense units of the armed forces, normally organized under a cyber force constituting military cyber defense and can be supported by other State powers if necessary (political, economic, diplomatic, etc.).

535. National cyber defense is a fundamental part of national defense, supporting it in the fulfillment of the mission, contributing to the credible level of deterrence, facilitating cooperation with international organizations, allowing efficient use of resources, minimizing risks to civilian population and its own forces, promoting national defense awareness (cyber defense awareness campaigns, cyber reserve) and cooperating with the private and academic sectors.

536. To achieve robust national cybersecurity, it is necessary to strengthen the three pillars (cyber resilience, cyber protection and cyber defense), as well as to keep close collaboration and cooperation between them and with their international counterparts.

537. Strong national cybersecurity needs a national cybersecurity strategy that is clear (expressed in understandable language at all levels), accurate (setting out effective guidelines and measures tailored to the national situation), realistic (setting concrete achievable goals), and practice (foreseeing the necessary resources for implementation).

538. A national cybersecurity strategy should identify the target end state, define a specific governance model that includes all major national actors, assess main cyber risks to national security, establish concrete measures to mitigate expected cyber risks, facilitate applying the measures with the provision of the necessary resources, and monitoring compliance with and effectiveness of the measures through the establishment of a indicators system.

539. There are some general references for the formulation of a national cybersecurity strategy, such as the "Guide to Developing a National Cybersecurity Strategy"[51] of the ITU and other organizations or the "National Cyber Security Strategy Guidelines"[52] of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE).

540. There are numerous national references (Brazil, China, Estonia, France, Israel, United Kingdom, United States, Spain, etc.), with different approaches, which can serve as examples. Studies on the organization of cybersecurity in these countries can be found on the NATO CCDCOE website.[53]

541. The development and implementation of a national cybersecurity strategy is a cyclical process comprising five phases: *initiation, analysis, strategy production, implementation and monitoring.*

FIGURE 31. CYBER SECURITY STRATEGY CYCLE

542. In the *initiation phase,* a management team is formed in order to devise and monitor the implementation of the strategy. The management team is made up of a director, national experts and all the public and private sector national actors, whose participation and collaboration are necessary at some stage of the process.

543. In the *analysis phase,* the current situation is examined, the target end state is determined, a risk analysis is performed to assess cyber risk to reach the target end state, different national strategies with different approaches and experience are analyzed and evaluated to contrast ideas and lastly, the potential measures to be implemented are analyzed and evaluated.

544. In the *strategy production phase,* a draft strategy is prepared according to the outcome of the analysis phase and it is distributed to all the actors involved, public and private, to try to reach a national consensus that is as extensive as possible. Once an acceptable consensus is reached, the draft is consolidated and submitted as a final document for approval and publication.

545. In the *implementation phase,* the strategy is materialized according to an action plan that establishes the courses of action, specific objectives, responsible entities, schedule and mechanisms and providing the necessary human and financial resources.

546. Finally, in the *monitoring phase,* the management team monitors compliance with the measures defined in the strategy and assesses the effectiveness of the measures implemented (with periodic audits), identifying the maturity level reached and the takeaways that help improve the process.

547. One of the most important aspects of national cybersecurity is the *protection of critical infrastructures* against cyber threats.

548. The protection of critical infrastructures is the responsibility of critical infrastructure operators (the vast majority of which are private sector) that implement the cybersecurity that they consider appropriate, without interruptions, which is the usual in periods of peace or stability.

549. Cybersecurity pre-established by critical infrastructure operators is usually not enough to protect against sophisticated cyber attacks that affect national security, so procedures must be provided, within the framework of national cybersecurity, to prepare additional cybersecurity measures to compensate for the shortcomings in severe cases. These compensation mechanisms can occur with forecasting and reserving additional economic or human resources.

550. The cyber force must be prepared, in case of a national need, to provide specific support to the assigned critical infrastructure operators, through operational and technical capabilities; in particular, security events management, audits, digital forensics and deployable cyber defense.

International cybersecurity

551. Many of the cybercrimes and cyberattacks that affect citizens, entities, or the interests of a nation come from territories or means belonging to other nations. Furthermore, the technical and legal attribution of the origin of cyber attacks is difficult to identify without the collaboration of the countries involved in the cyber attack route. For all these reasons, *no country in the world is self-sufficient to prevent and prosecute all the cybercrimes and cyberattacks* that affect it. Consequently, international cooperation in cybersecurity is vital not only for solid international cybersecurity, but also for national cybersecurity.

552. International cybersecurity is fundamentally based on *cooperation* between the entities responsible for each of the pillars of national cybersecurity (cyber resilience, cyber protection and cyber defense) and their counterparts from other countries and international organizations.

553. It is necessary to establish *political and diplomatic agreements* between countries and international organizations for the persecution of cyber attacks and cybercrimes; and reach the widest possible consensus on the application of international law in cyberspace.

554. In the context of *cyber resilience,* it is important that all national public or private CERTs be officially recognized and actively participate in international forums and organizations dedicated to coordinating CERTs around the world or in a specific geostrategic area for the purpose of sharing information on cyber vulnerabilities, cyber attacks and cyber risk, and the corresponding mitigation measures.

555. Worldwide, the FIRST (Forum of Incident Response and Security Teams) stands out as the predominant initiative in the coordination of national CERTs.

556. At a European level, the European Union Agency for Cybersecurity (ENISA) looms large. ENISA aims to actively contribute to European cybersecurity policy, supporting European Union Member States and stakeholders in responding to large-scale cross-border cyber incidents in cases where two or more EU member States have been affected. Furthermore, ENISA contributes to the proper functioning of the digital single market.

557. ENISA works closely with Member States and the private sector to offer advice and solutions, as well as to improve their capacities, including, pan-European cybersecurity exercises, development and evaluation of national cybersecurity strategies, cooperation and development of CERT capabilities, studies on the Internet of Things and smart infrastructures and cyber threat analysis.

558. The main coordinating bodies for European CERTs are the TF-CSIRT Trusted Introducer and the European Government CERTs (EGC) Group.

559. At the inter-American level, the Latin American and Caribbean Internet Address Registry (LACNIC[54]) is prominent. LACNIC contributes to regional Internet development through an active cooperation policy; it promotes and defends the interests of the regional community; and it helps create conditions for the Internet to be an effective instrument for social inclusion and economic development in Latin American and the Caribbean. The annual meetings of CSIRTs (LAC-CSIRTs[55]) and the Amparo Project[56] are noteworthy.

560. In the context of cyber protection, it is important that national cybercrime and cyberterrorism units of police departments cooperate with their counterparts in other countries and international organizations.

561. At the European level, it is essential for national cybercrime units to have a relationship, coordination and cooperation with EUROPOL's European Cybercrime Centre (EC3[57]) aimed at strengthening the law enforcement response to cybercrime in the EU and thus to helps protect European citizens, businesses and governments from online crime.

562. Also important is the relationship, coordination and cooperation with the European Union Agency for Criminal Justice Cooperation (Eurojust[58]) the purpose of which is to help the European authorities cooperate in the fight against terrorism and serious forms of organized crime that affect more than one EU country.

563. At the inter-American level, the relationship, coordination and cooperation of national cybercrime units with the branch responsible for the fight against cybercrime in the Police Community of the Americas (Ameripol) is essential. It is aimed at promoting, strengthening and systematizing police cooperation, information exchange and legal assistance between member States.

564. In the context of cyber defense, it is important for the national cyber force to cooperate with other cyber forces in its geopolitical environment and with the international collective defense organizations to which it belongs (*NATO, Inter-American Defense Board,* etc.).

565. It is also necessary to actively participate in international cyber defense forums such as the *Cyber Commanders Forum,* initially founded by countries belonging to the NATO CCDCOE and currently open to other nations, which aims to promote international cooperation in cyber defense; or the *Ibero-American Cyber Defense Forum* (Foro Iberoamericano de Ciberdefensa) founded in 2016 and currently formed by Argentina, Brazil, Chile, Colombia, Spain, Mexico, Peru and Portugal, in order to ensure fluid cooperation in cyber defense, especially in the fields of training, exercises, information exchange and research and development.

566. International cooperation in cyber defense is usually more easily achieved in those aspects related to defensive activities than in those related to intelligence and offensive activities. In the latter, it is necessary to lay the foundations for cooperation, gradually, through bilateral agreements with partners with whom a solid level of mutual trust has previously been gained.

Public-private partnership

567. The military industry used to be the engine and benchmark of civilian industry that took advantage of the dual-purpose military research and development. Currently the trend is different, the large multinational corporations along with the universities are making the great technological contributions which feed the military establishment. Many of the technologies developed in the information technology, cybersecurity, video games and social network sectors are very useful in the field of military cyber defense.

568. The establishment of a *national cyber defense industry* is essential to avoid dependence on other countries in developing and employing critical cyber defense capabilities.

569. In order to develop a national cyber defense industry, it is necessary that the defense ministry promote and establish *cyber defense capability development and procurement programs* including cyber weapons systems (as it does in land, sea and air domains) through agreements and consortia with the main national companies and corporations.

570. Cyber defense capability development and procurement programs have to be defined with special care to ensure a *balance of interests* of the two parties. On a one hand, the use, evolution and customization of the products by the armed force cyber defense units should be guaranteed under the conditions that the ministry requires, and the sales to other countries without ministry authorization must be limited. On the other hand, the necessary financial profit of the companies should be facilitated, allowing the marketing of the products according to predetermined conditions.

571. In most cases, it will be necessary that the *intellectual property* of the products developed in cyber defense programs, financed by the Ministry of Defense, remain with it.

572. *Public-private partnership* must avoid becoming a zero-sum game[59] and work to reach models that ensure win-win situations against common cyber threats. This can be attained with the establishment of higher intelligence with data provided by the private sector (optimized data on cyber threats, cyber vulnerabilities and cyber risks from its extensive global networks) and the intelligence and analysis capacities of high-level political and strategic levels of the public sector.

573. For an effective information exchange between the private and public sectors, it is necessary to build *mutual trust* and an effective mechanism to ensure that the contribution of both parties is equal; that the information is not leaked to third parties without authorization; and that both parts make appropriate use of the information.

574. Public-private partnership is essential to improve cybersecurity and cyber resilience critical infrastructures, establishing joint mechanisms to prevent and respond to advanced cyber threats that have the ability to evade cybersecurity implemented by the operators of the critical infrastructures.

575. Public-private partnership in cyber defense is necessary for the following reasons:

- It achieves a more effective and efficient national cybersecurity, creating situations of common benefit and avoiding situations of competition and duplication of efforts.
- It minimizes the cyber risk surface of the two sectors by enjoying a more robust common cybersecurity structure.
- It facilitates the scope and application of the measures established in the national cybersecurity strategy, which in many cases must be implemented by private sector actors.
- It is able to respond jointly and quickly to a cybercrime or cyber attack that affects national security.
- It raises awareness in the private sector of its fundamental role in national security over its commitment to clients.
- It ensures compliance with national cybersecurity regulations.
- It saves costs by efficient resource sharing.
- It accesses a more complete information and knowledge database.

576. Public-private partnership in cyber defense requires the active participation of, at least, the national cyber force; the national intelligence services; National CERTs; critical operators; public procurement branches; crisis management agencies; regulatory bodies; judicial services; technology observatories, think tanks, foundations, and public and private research and development centers related to cyber defense; and universities and private companies.

577. According to a study carried out by ENISA, the *most in-demand services* in public-private partnership in cyber defense are information exchange (83%), research and analysis (62%), awareness (62%) and early warning (59%). Other common services are crisis management, standards and good practice guides, contingency and continuity plans, security audits, cyber exercises, market research, statistics, strategy planning and risk analysis.

578. There are four approaches to public-private partnership in cyber defense: foundational cooperation, preventive cooperation, reactive cooperation and comprehensive cooperation.

579. *Foundational cooperation* focuses on research and development of cyber defense systems, products, tools and TTPs based on a joint or agreed strategy and agenda.

580. *Preventive cooperation* focuses on establishing a cyber defense system to anticipate, prevent, detect, protect and alert on cyber attacks from common threats.

581. *Reactive cooperation* focuses on the establishment of a cyber defense system to react to cyber attacks from common threats and restore operations.

582. *Comprehensive cooperation* focuses on the implementation of a full-spectrum cyber defense environment that implements, coordinately, the three areas (foundational, preventive, reactive) and establishes feedback mechanisms between them.

Third-party risks

583. Most cyber defense systems and capabilities use components (hardware, software, firmware) that rely on third parties (vendors, supply chain, support, consultants) for their manufacture, supply, distribution, start up, operation, and maintenance.

584. The list of *third parties* that can jeopardize an organization includes hardware component manufacturers, software and firmware developers, integrators, carriers, subcontractors, resellers, end suppliers; technical supports for installation, commissioning and maintenance; and consultants and professional services for operation, customization or updating.

585. *Third-party risk management* is of such complexity, detail and extent that it must be carefully and realistically planned, avoiding unattainable or unprofitable objectives for the organization. However, third-party risk, and in particular the supply chain risk, is recognized as one of the great current threats that any organization must face and properly manage.

586. Large national organizations and corporations have an ability to control third parties–which is not accessible to medium or small organizations–such as having a certain control in the manufacturing chain, having access to the software source codes or requiring specific security controls to all third parties involved. For this reason, it is important that the management of third parties be centralized in the body with the greatest competence, and consequently, can pull more weight when imposing measures on third parties.

587. Third-party risk management aims to ensure, as far as possible, that the products, systems and services perform exactly as expected (in accordance with the technical and operational requirements), not going beyond what was purchased, and not being enabled to do anything else in the future (free of back doors, pre-installed malware, etc.).

588. Some products, services or processes may require a nationally or internationally recognized quality or security certification; but in many cases this is not feasible or profitable, so a realistic third-party risk management must be carried out.

589. In some cases of critical cybersecurity components or systems (cryptographic algorithms, SIEM, threat hunting, advanced honey nets, etc.), the intellectual property, design, manufacturing, support and maintenance may be required to reside in a national company or corporation or in an allied nation. However, in today's globalized and dynamic market, where companies easily change ownership or switch countries to ones that have different geopolitical positions, this measure is usually not effective in the medium and long term.

590. Third-party risk management prevents the acquisition of products, systems or services with shortcomings, hidden faults or with pre-installed malicious mechanisms. Once products are purchased and installed or services are provided, there are two common ways to verify that they are operating properly: white-box and black-box testing.

591. In *white-box testing,* internal details of the product (scheme, design, source code, etc.) are studied, and with the information obtained, tests are designed to verify operation and behavior. This testing is only possible if the manufacturer provides the proper information, which in many cases is not possible for fear of information leaking to potential competitors. Only large customers or organizations, that can guarantee confidentiality and that can provide the manufacturer with benefits higher than the risk of leakage, would be able to obtain the necessary white information.

592. In *black-box testing,* internal details of the product are ignored, and operation and behavior are studied through a test protocol based on specially designed inputs that require a specific output.

593. *A third-party management process* requires six phases: definition and establishment of the management team, preparation and implementation of the awareness plan, its own IT inventory analysis, third-party inventory development, action plan, and assessment.

594. *The risk management team* must direct the entire management cycle, from awareness to assessment. It must be made up of experts in the cybersecurity of the organization's systems, products and services, quality control, hiring processes and legal issues.

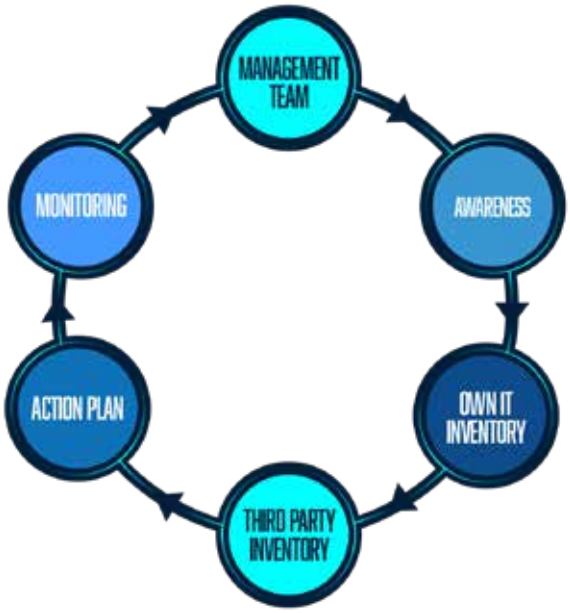


FIGURE 32. THIRD PARTY RISK MANAGEMENT

595. In most cases, it will be necessary to develop and implement a third-party *risk awareness plan* geared towards senior leaders, since, despite the fact that third-party risk can have serious consequences for the organization, it is either usually non-occurring or not perceived in an obvious or evident way.

596. *Its own IT inventory* provides essential information to identify current third parties in support and maintenance tasks and potential future third parties (manufacturers, suppliers and distributors).

597. *A third-party inventory* identifies current and potential third parties (manufacturers, suppliers, distributors, carriers, support and maintenance services for systems and services critical to the organization) and possible security breaches throughout the process (manufacturing, transportation, distribution, provision, implementation, start up, operation, update, evolution, customization and maintenance).

598. An action plan details the concrete measures to be implemented, based on a realistic and efficient strategy. Some aspects to consider are non-disclosure agreements (NDA), vulnerability reporting agreements, employee background checks, accreditation or certification of third parties or their products as a requirement in hiring processes, cybersecurity requirements throughout the hiring cycle from design to commissioning, reviews of compliance with cybersecurity measures by third parties, advice by third parties on the security of the systems provided, possibility of remote support, requirement of periodic tests, security audits, service level agreements (SLAs) and good practice guides.

599. There are numerous possible measures aimed at managing third parties, mainly hiring and technical. *ISO 28000 standard* is a good reference to identify suitable measures for the organization.

600. During the *assessment phase,* compliance and effectiveness of the measures must be assessed and fed back to the entire cycle in order to gradually improve the action plan and align it with the organization's strategic objectives.

Cyber risks in pandemics

601. A global pandemic declaration by the World Health Organization (WHO) results in measures taken by governments of affected nations that carry additional cybersecurity risks.

602. People residing in territories affected by a pandemic focus all their attention on health prevention and *lighten their individual cybersecurity responsibilities,* taking for granted any communication, message, email, link they receive in relation to the pandemic without carrying out any type of verification. This individual relaxation is noted by cyber criminals and consequently, escalate their criminal activity.

603. During pandemic situations, *information is oversaturated,* making it difficult for users to assimilate and filter it. Also, information oversaturation can lead to network collapse.

604. Pandemic situations may require the population's confinement and an outcome is *hyperactivity in social media sites* that, together with loosening the employment of individual cybersecurity measures, generate a *cybercrime pull factor* on social media environments.

605. One of the great problems of modern societies is *disinformation* (hoaxes, fake news, influence). During pandemic situations, information oversaturation predominates; any information that seems to come from an official source tends to be considered reliable, and hyperactivity in social networks thrives. All these factors create the ideal conditions for fake news to spread easily and quickly.

606. Many countries affected by a pandemic take measures to contain the virus spread that require the cessation of non-essential activities and the confinement of non-essential workers at home. This leads many companies and organizations to promote *telecommuting* and, to this end, create remote accesses to their information and control systems without due planning or preparation, and not taking into account the cybersecurity risks entailed.

607. Telecommuting carries cyber risks that must be carefully studied and reconciled with potential operational benefits. The risk is as high for small companies–usually unprepared to institute secure remote accesses–as it is for large organizations or corporations, with very robust cyber security systems that are constantly being watched by competitors or adversaries looking for vulnerabilities that would grant them access. Remote accesses are surely one of the main penetration routes that criminals will endeavor to attack.

608. An example of an attack via remote access to a large business was the 2011 cyberattack against Lockheed Martin Corporation, a defense company, where cyber attackers exploited the VPN[60] access system, which was used by employees to log in remotely using secure access mechanisms (RSA SecurID hardware tokens).

609. In *confinement situations,* in most cases, IT system security administrators will be considered non-essential and will be forced not to carry out their duties on-site and perform their work from home, using remote accesses, thus weakening cybersecurity at all levels.

610. One of the measures that some countries implement to contain the spread of the virus is the use (usually on a voluntary basis) of *mobile applications* in order to identify, isolate, test and treat each case of infection; know the traceability of the disease; create epidemiological intensity maps; and control mobility. These applications can be considered legally invasive because they require the use of specially protected data such as health, personal and geolocation data. In these cases, national cybersecurity must guarantee privacy rights and ensure the legitimate use of data, exclusively for purposes of epidemiological containment and protect them against unauthorized access.

Information

611. *Information* is one of the main components of the cyber ecosystem, because cyberspace is an ideal environment for preparation, presentation, storage, processing, transport and destruction.

612. In cyber defense, there are four relevant aspects to consider in relation to information: its own information and knowledge management and actions against adversary's information and knowledge management; protection of confidentiality, integrity and availability of its own information and the action against confidentiality, integrity and availability of the adversary's information; protection against unauthorized exfiltration attempts of its own information and cyber operations against adversaries in order to exfiltrate information useful to the mission; and influence and countering influence operations.

613. Its own *information and knowledge management* is an essential command capability that the cyber force must promote and protect.

614. *An action against the adversary's information and knowledge management* produces strategic effects. For example, actions that affect the veracity of the cyber situational awareness or actions that affect the integrity of operational plans can create mistrust in the command and control system and consequently severely affect decision-making. This responsibility is typical of information operations units, but the cyber force can provide support due to its special preparedness to operate in cyberspace.

615. *Protecting the confidentiality,* integrity and availability of information is a service of the cyber force, subordinated to the MoD information assurance branch.

616. *Actions against the protection of confidentiality and integrity of the adversary's information* are more typical of crypto services using cryptanalysis techniques, nevertheless the cyber force can support them, if necessary. Actions against availability are characteristic of the cyber force in offensive actions such as DDoS cyber attacks.

617. *Protecting against unauthorized exfiltration of information* is a responsibility of the cyber force, primarily through its cyber threat hunting capability.

618. *Cyber operations in order to exfiltrate information* of adversaries is a responsibility of the cyber force that must be carried out with extreme care and which will require the involvement of cyber exploitative and offensive capabilities.

619. *Influence operations* are aimed at preparing, managing, modifying, denying, presenting, destroying or using public or adversary information, to promote perceptions, attitudes and behavior in certain audiences, favorable to its own operations and thus influence the decision-making, both human and automated. It is a responsibility more proper to the information operations (INFOP) and psychological operations (PSYOP) units.

620. Because cyberspace is currently the primary means for information handling, the cyber force can provide important support to INFOP and PSYOP units in influence operations due to its knowledge of the domain and preparedness to operate in it.

621. *Countering influence operations in its own networks* requires control of its own cyberspace (cyber supremacy or cyber superiority), a robust level of protection of its own information confidentiality, integrity and availability and an individual awareness of associated risks and vulnerabilities.

622. *Countering influence operations in public networks* is a highly complex problem that requires the collaboration of private organizations and permanent awareness throughout the organization of the associated risks and vulnerabilities.

623. In most cases, information operations and influence operations will require joint action between INFOP units, PSYOP units and the cyber force.

624. In the national cybersecurity context, *disinformation* actions are very common in order to change the opinion of a target audience on a specific matter, replacing it with another alternative vision; and they are considered by the political powers as one of the main threats they face.

625. The resolution of disinformation problems goes beyond the implementation of purely technical measures and it needs to reconcile legal aspects, in particular freedom of expression, which are beyond the scope of military cyber defense. However, the cyber force can support the implementation of technical measures.

LEGAL ISSUES

626. The *application of international law to cyberspace and cyber operations* has been a matter of debate in the last decade and it continues to be so today. During this debate, two main positions have emerged, the Western and the Eastern.

627. *The Western position,* supported by the European Union and NATO nations, advocates that current international law is applicable in cases of cyber attacks and cybercrime, with the corresponding interpretation; and consequently, the preparation of a specific international law for cyberspace matters is unnecessary.

628. *The Eastern position,* supported mainly by Russia and China, advocates that the development of a specific law for cyberspace issues is necessary and States must have sovereign control over their cyberspace.

629. Due to the cross-border nature of cyber attacks and cybercrime, the ability to prosecute offenders or cyber attackers in the national legal system is very limited and therefore it is very important to reach an *international consensus.*

630. Currently, there is *majority support for the Western position,* endorsed by the UN, NATO, the European Union and the countries participating in the Tallinn Manual, and it is considered that international law does apply to criminal and malicious actions in cyberspace, moving the debate to how international law applies in cyberspace.

631. Currently the debate is focused on the application of each of the most relevant aspects, using the topics and rules considered in the *Tallinn Manual 2.0* as a basis: general international law and cyberspace (sovereignty, due diligence, jurisdiction, law of international responsibility, cyber operations not per se regulated by international law), specialized regimes of international law and cyberspace (international human rights law, diplomatic and consular law, law of the sea, space law, international telecommunication law), international peace and security and cyber activities (peaceful settlement, prohibition of intervention, the use of force, collective security) and the law of cyber armed conflicts (the law of armed conflict generally, conduct of hostilities, certain persons, objects, and activities, occupation, neutrality).

632. In some cases, consensus is widespread, as in the prohibition of intervention or the right to self-defense; in others, there is still a disparity of criteria as in sovereignty and due diligence.

633. There is still a division between NATO-EU nations and the SCO nations (The Shanghai Cooperation Organization: China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, India and Pakistan) on whether existing treaties and customary law are suitable or not. While NATO/UE nations consider that the existing regulation is adequate, the SCO nations argue the opposite.

634. As cyberattacks from State-sponsored APTs become more frequent, States feel the need to face them through appropriate response or coercive measures in any field, technical, military, political, diplomatic, economic, or through any other State power. For this, *an attribution (clear and undisputed) to a State is necessary.*

635. Many States recognize that the proliferation of APT cyber attacks is largely due to the difficulty of achieving attribution according to traditional court evidentiary standards. Consequently, more States are progressively considering attribution in cyberspace a political decision based on technical and intelligence analysis of numerous facts that corroborate a specific authorship.

636. This new legal approach for attribution in cyberspace would empower States to defend themselves against cyber aggressions from other States and diminish their disadvantage where States are victims of cyber attacks due to a legal artifice.

637. Another problem that States face in responding to cyber aggressions from other States is that the aggressor triggers *low-intensity long-lasting cyberattacks,* in such a way that, in the

long term, they cause serious effects, but specifically never exceed the threshold necessary to be recognized internationally as armed attacks, thus avoiding the response through legitimate retaliatory actions. In this case, the debate focuses on the search for legal actions that lead to sanctions for the aggressor State.

638. *Collective response* to aggression against an alliance member nation is a legally controversial matter, despite collective defense organizations such as NATO considering this possibility. The invocation of Article 5 of the Washington Treaty in the case of a cyber attack would be considered on a case-by-case basis.

639. It is accepted, by a vast majority of countries, that a cyber operation that causes serious damage to national interests can be considered an *armed attack,* even in the absence of human casualties, and consequently the right to self-defense can be applied and legitimate and proportionate military retaliation can be unleashed from any domain, traditional or cyberspace.

640. Steps are currently being taken to promote non-binding international standards for responsible behavior in cyberspace, although, at the moment with little success, since there are many views on what a responsible behavior model should be.

641. Despite the difficulty of the challenge, initiatives such as the *Paris Call for Trust and Security in Cyberspace of 2018*[61] invites all cyberspace actors to work together and it encourage States to cooperate with private sector partners, the world of research and civil society. The supporters of the Paris Call commit to working together to adopt responsible behavior and implement the fundamental principles in cyberspace which apply in the physical world: protect individuals and infrastructure, protect the Internet, defend electoral processes, defend intellectual property, non-proliferation, lifecycle security, cyber hygiene, no private hack back, and international norms.

642. Regarding the use of cyber offensive operations by the armed forces in armed conflicts or in peacekeeping operations, the legal debate continues on issues such as the limits on State sovereignty, the threshold of armed attack that provokes the right of self-defense, the application of the rules of international humanitarian law, the definition of legal mandates for cyber forces or the rules of engagement.

643. Offensive cyber operations remain a controversial issue in many countries, despite the fact that it is globally recognized that they are subject to the same rules and principles of international law as traditional military operations.

644. Offensive cyber operations are considered by NATO through the mechanism called SCEPVA[62] through which the commanders of NATO operations will be able to have cyber effects available, provided voluntarily by the NATO nations.

645. Renowned experts in international law *warn* that the law protects the commander that chooses to use offensive cyber operations instead of traditional ones in those cases where the use of cyber operations is considered to cause the same military effects as traditional operations, but with a lower risk of collateral damage (especially to civilians) and its own forces. Instead, the commander who chooses traditional operations despite the greater risk of collateral damage and to its own forces could suddenly be in a legally difficult justification situation.

646. The applicability of *international humanitarian law* in cyber operations is supported by most countries; however, there is a small group of countries that question it as they consider that this could imply a militarization of cyberspace.

647. The Tallinn Manual 2.0 is currently the world reference in the application of international law to cyber operations; however, it is reminded that it is a recommendation and not a binding norm.

STANDARDS

648. Military cyber defense is developed through a doctrinal body that establishes norms, criteria, principles, procedures, guidelines, recommendations and good practices in the design, execution and planning of military operations in cyberspace.

649. International references regarding cyber defense doctrine are scarce. NATO, habitual doctrinal reference for allied nations, has recently approved its AJP-3.20 "Allied Joint Doctrine for Cyberspace Operations", which describes some basic aspects of cyber defense.

650. Nations are reluctant to share their cyber defense doctrines, especially regarding intelligence and offensive activities, which forces nations to get involved in the preparation of their own doctrinal body.

651. In practice, associations such as ISO or NIST develop global standards circumscribed to cybersecurity or security of information and telecommunications systems, which would cover a small part of the cyber defense field.

652. The International Organization for Standardization (ISO) has a standards family dedicated to information security management systems (*ISO/IEC 27000 family*[63]), in which the ISO/IEC 27001 stands out as a standard that specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.

653. The ISO standards have the disadvantage that they are not freely accessible (pay standards) and this deters the freedom of sharing, consultation and distribution that is required for their study, implementation and monitoring, in direct contradiction to the spirit of standardization, to reach all stakeholders in an agile and effective way.

654. The US National Institute of Standards and Technologies (NIST) has a standards family dedicated specifically to cybersecurity[64], highlighting the standard dedicated to the *"Cybersecurity Framework"*[65] that provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders; it facilitates the identification and prioritization of actions to reduce cybersecurity risk; and it aligns policy, business, and technological approaches to managing that risk.

655. Another NIST reference in cyber defense is the NICE[66] (National Initiative for Cybersecurity Education) framework, a joint initiative between the United States government, academia and private sector in order to stimulate and promote a cybersecurity education, training and education ecosystem.

656. The NIST standards, although they are federal standards of the United States, are, de facto, internationally accepted and reputable standards and have the advantage that they are freely accessible, which facilitates the work of standardization. In particular, cybersecurity standards stand out for clarity, organizational order and the inclusion of online training.

657. The National Cryptography Center of Spain *(CCN-CERT)* has a complete set of information technology and telecommunications security guides (STIC guides[67]), in Spanish, and many of them are freely accessible. In addition to the *STIC guides*, they have a quite complete set of STIC tools[68] and training[69]. The *EAR/PILAR*[70] tools are worth highlighting, for the analysis and risk management of an information system following the MAGERIT[71] methodology (official in Spain and NATO).

658. Other cybersecurity standards of fine repute are those developed by Germany's Federal Office for Information Security (BSI) which can provide another useful vision.[72]

ACRONYMS

AMERIPOL	Police Community of the Americas (Comunidad de Policías de América, in Spanish)
APT	Advanced Persistent Threat
BSI	Federal Office for Information Security of Germany
ByOD	Bring your Own Device
CCN	National Cryptographic Center of Spain (Centro Criptológico Nacional de España, in Spanish)
CERT	Computer Emergency Response Team
CIS	Communication and Information System
CKT	Cyber Key Terrain
CNO	Computer Network Operations
CRAMM	CCTA Risk Analysis and Management Method
CSA	Cyber Situational Awareness
CSIRT	Computer Security Incident Response Team
CyOC	Cyberspace Operations Centre
DNS	Domain Name System
EAR	Risk Analysis Environment (Entorno de Análisis de Riesgos, in Spanish)
EC3	European Cybercrime Center
ENISA	European Union Agency for Cybersecurity
EUROJUST	European Union Agency for Criminal Justice Cooperation
EUROPOL	European Union Law Enforcement Agency
FIRST	Forum of Incident Response and Security Teams
FOC	Full Operational Capability
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
IXP	Internet Exchange Point
LACNIC	Latin America and the Caribbean Network Information Centre
MAGERIT	Information Systems Risk Analysis and Management Methodology (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, in Spanish)
MISP	Malware Information Sharing Platform
NATO CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
NDA	Non-Disclosure Agreement
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology of the US Department of Commerce
NOC	Network Operations Centre
OCTAVE	Operationally Critical Threat Asset and Vulnerability Evaluation
OSINT	Open Source Intelligence
PILAR	Impact Analysis and Continuity of Operations Tool
RAE	Royal Academy of the Spanish Language (Real Academia Española, in Spanish)
RAT	Remote Administration Tool
RFI	Request for Information
RPAS	Remotely Piloted Aircraft System
SCEPVA	Sovereign Cyber Effects Provided Voluntarily by Allies
SCO	The Shanghai Cooperation Organisation
SIEM	Security Information and Event Management
SLA	Service-Level Agreement
SOC	Security Operations Centre
TCP	Transmission Control Protocol
TOR	The Onion Router
TTP	Tactics, Techniques, and Procedures
UAV	Unmanned Aerial Vehicle

REFERENCES

- **ACT Report on NATO Cyber Defence Taxonomy and Definitions** [Report]. - 2014.
- **AJP.3 Allied Joint Doctrine for the Conduct of Operations** [Book]/auth. NATO Standardization Office (NSO). - 2019.
- **CCN-STIC-480F Seguridad en el controls de procesos y SCADA** [Book]/auth. CCN-CERT. - 2009.
- **Ciberamenazas y tendencias** [Report]/auth. CCN-CERT. - 2019.
- **Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio** [Book]/auth. autores varios. - [s.l.] : Instituto Español de Estudios Estratégicos, 2010.
- **Cooperative Models for Effective Public Private Partnerships** [Report]/auth. ENISA. - 2011.
- **Cyber attack Trends** [Report]/auth. Check Point. - 2019.
- **Cyber Commanders Handbook v1.0 (DRAFT)** [Book]/auth. NATO CCDCOE. - 2019.
- **El Manual de Tallin y la Aplicabilidad del Derecho Internacional a la Ciberguerra** [Journal]/auth. Galizia Roberto Claudio.
- **Framework for Improving Critical Infrastructure Cybersecurity** [Book]/auth. NIST. - 2018.
- **Guide to Developing a National Cybersecurity Strategy** [Book]/auth. Co-publication of 12 partner organisations facilitated by ITU. - [s.l.] : NATO CCDCOE, 2018.
- **International Cyber Norms: Legal, Policy & Industry Perspectives** [Book]/auth. Anna-Maria Osula Henry Rõigas (Eds.). - [s.l.] : NATO CCDCOE, 2016.
- **Internet Attacks: A Policy Framework for Rules of Engagement** [Journal]/auth. William Yurcik David Doss // Illinois State University.
- **ISO/IEC 27000 Information security management systems — Overview and vocabulary** [Book]. - 2018.
- **ISO/IEC 27001 Information Security Mangement** [Book]. - 2018.
- **IT Security Predictions** [Report]/auth. Splunk. - 2020.
- **Joint Doctrine for Military Cyberspace Operations** [Book]/auth. Royal Danish Defence College. - 2019.
- **JP 5-0 Joint Planning**/auth. USA Defence Staff. - 2017.
- **Key Terrain in Cyberspace** [Journal]/auth. David Raimond Gregory Conti, Tom Cross, Michael Nowatkowski. - 2014.
- **La Ciberdefensa: un nuevo frente una nueva necesidad** [Journal]/auth. Javier López de Turiso Néstor Ganuza. Roberto Gil, Félix Estrada, Joaquín Corominas // Revista Aeronáutica num 817. - 2012.
- **M-Trends** [Report]/auth. FireEye. - 2019.
- **National Cyber Security Organisation in Israel** [Book]/auth. Housen-Couriel Deborah. - [s.l.] : NATO CCDCOE, 2017.
- **National Cyber Security Organisation in United States** [Book]/auth. Piret Pernik Jesse Wojtkowiak, Alexander Verschoor-Kirss. - [s.l.] : NATO CCDCOE, 2016.
- **National Cyber Security Organisation Spain** [Book]/auth. Cendoya Alexander. - [s.l.] : NATO CCDCOE, 2016.
- **National Cyber Security Organisation: Estonia** [Book]/auth. Osula Anna-Maria. - [s.l.] : NATO CCDCOE, 2015.
- **National Cyber Security Organisation: France** [Book]/auth. Brangetto Pascal. - [s.l.] : NATO CCCOE, 2015.
- **National Cyber Security Organisation: United Kingdom** [Book]/auth. Osula Anna-Maria. - [s.l.] : NATO CCDCOE, 2015.
- **National Cyber Security Organization: Czechia** [Book]/auth. Tomáš Minárik Taťána Jančárkov. - [s.l.] : NATO CCDCOE, 2019.
- **NATO ACO Cyber Defence Functional Planning Guide** [Report].
- **NATO AJP 3-20 Allied Joint Doctrine for Cyberspace Operations version 1 (DRAFT)** [Book].
- **NIPP National Infrastructure Protection Plan** [Book]/auth. CISA/US Department of Homeland Security . - 2013.
- **OM 10/2013 Creación del Mando Conjunto de Ciberdefensa**/auth. Ministerio de Defensa de España. - 2017.
- **On Cyber Defence** [Journal]/auth. Ali Col Rizwan.

- **Overview of the UN OEWG developments: continuation of discussions on how international law applies in cyberspace** [Book]/auth. Tolppa Maria. - [s.l.] : NATO CCDCOE, 2020.
- **PDC-01(A) Doctrina para el Empleo de las FAS**/auth. Ministerio de Defensa de España. - 2018.
- **Public Private Partnership in a NATO Context** [Report]/auth. NATO STO. - 2019.
- **Strategic importance of, and dependence on, undersea cables** [Book]/auth. Henrik Beckvard (Ed.) Keiko Kono. - [s.l.] : NATO CCDCOE, 2019.
- **Tallinn Manual 2.0** [Book]. - 2017.
- **The NATO Policy on Cyber Defence: The Road so Far** [Journal]/auth. Gergely Szentgáll. - 2013.
- **The next phase of russian information warfare**/auth. Giles Keir.
- **The Tallinn Manual 2.0** Highligths and Insights [Journal]/auth. Jensen Eric Talbot.
- **Threat Landscape** [Report]/auth. ENISA. - 2018.
- **Trends in International Law for Cyberspace** [Book]/auth. Kaska Kadri. - [s.l.] : NATO CCDCOE, 2019.
- **UNE-ISO 28000: especificación para sistemas de gestión de seguridad de la cadena de suministros** [Report]. - 2008.

NOTES

[1] NATO Bi-SC Initial Assessment of Recognising Cyberspace as a Domain

[2] MAGERIT is the risk analysis and management methodology developed by the Spanish Higher Council for Electronic Administration (Consejo Superior de Administración Electrónica de España).
[3] PILAR is the risk analysis tool developed by the CCN-CERT that facilitates the application of the MAGERIT methodology.
[4] CRAMM, risk analysis methodology developed by the British CCTA (Central Computer and Telecommunication Agency).
[5] OCTAVE (Operationally Critical Threat Asset and Vulnerability Evaluation), risk analysis methodology developed by the Carnegie Mellon University CERT.
[6] Zero-day cyber attack is a type of cyber attack that occurs by exploiting an unknown vulnerability or for which there is still no patch.
[7] EXPLOIT is piece of software code, a data chunk, or a script that exploits a bug or cyber vulnerability to cause an impact.
[8] PHISHING is a type of cyber attack aimed at deceiving a victim (simulating trustworthy sources for the victim, usually by email) in order to obtain confidential or private information (user, passwords, bank details, credit card details, etc.).
[9] SPEAR PHISHING is a type of cyber attack aimed at deceiving a group of specifically selected people (pretending to be a trustworthy entity for the victims) in order to obtain confidential information (usernames, passwords, bank details, credit card details, etc.) useful for carrying out a cyber operation.
[10] SPOOFING is a type of cyber attack that imhumantes a device or user on a network.
[11] PHARMING is a type of cyber attack in which web traffic is redirected to a fake site, exploiting software vulnerabilities in domain name systems (DNS) or in the users' computers.
[12] SNIFFING is a type of attack aimed at capturing traffic while it is being transmitted over the network, using a specific tool (sniffer), in order to analyze the network, obtain information or read communications.
[13] WATERING HOLE is a type of cyber attack aimed at deceiving a group of specifically selected people by infecting the websites they usually use in order to obtain useful confidential information to carry out a cyber operation.
[14] DENIAL of SERVICE ATTACK (DoS) is a type of cyber attack that seeks to make a machine, service or network resource unavailable to its legitimate users, by mass generation of superfluous requests in a short time looking to overload the system.
[15] DISTRIBUTED DENIAL of SERVICE ATTACK (DDoS attack) is a DoS attack using multiple different sources (usually using botnets).
[16] Man in the Middle (MitM) attack is a type of cyberattack in which a communication is intercepted, an interlocutor is supplanted and the other party is made to believe that communication is taking place with the authentic interlocutor.
[17] SQL INJECTION is a type of cyber attack in which malicious SQL (Database Query Language) statements are inserted into an entry field of a database-based website for execution.
[18] FLAME is a sophisticated modular malware (discovered in 2012) with the ability to spread to other systems across the network, record audio, capture screenshots, keyboard activity and network traffic, exploit devices connected by Bluetooth and make an external connection.
[19] STUXNET is a cyber weapon (discovered in 2010) designed to attack supervisory control and data acquisition (SCADA) systems. It is alleged to be responsible for the cyber attack on the Iranian nuclear platform.
[20] DUQU is a STUXNET-related cyber weapon that includes information stealing capabilities and, in the background, kernel drivers and injection tools.
[21] BLACK ENERGY is a toolkit (discovered in 2007) designed to generate distributed denial of service (DDoS) attacks.
[22] The Cyber Kill Chain® framework is a model developed by Lockheed Martin Corporation.
[23] OSINT, Open-source Intelligence
[24] SIEM (Security Information and Event Management) is a set of software tools that facilitates the management and correlation of events in order to provide organizations with useful information about potential threats.
[25] CERT: Computer Emergency Response Team

[26] CSIRT: Computer Security Incident Response Team
[27] https://www.first.org/
[28] https://www.trusted-introducer.org/index.html
[29] http://www.egc-group.org/
[30] Obfuscation is the deliberate modification of a computer program source code to make it difficult to understand keeping the original operation.
[31] SOFTWARE REVERSE ENGINEERING is a process of deconstruction of a piece of software to reveal its design, architecture, functions or extract knowledge.
[32] MACHINE LEARNING is a branch of Artificial Intelligence that studies computer algorithms that automatically improve through experience.
[33] BLOCKCHAIN is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a time stamp and transaction data.
[34] BIG DATA is a technology focused on the treatment of data sets too large or complex to be processed by traditional data processing software.
[35] 5G is the fifth-generation technology standard for cellular networks that provides higher bandwidth and faster speeds than the predecessor technology (4G).
[36] RPAS: Remotely Piloted Aircraft System
[37] RANSOMWARE is a type of cyber attack that threatens to publish the victim's data or permanently block access to them (usually through the encryption of the victim's files) if the victim does not agree to pay a ransom.
[38] WEBSITE DEFACEMENT is a cyber attack designed to change the visual appearance of a website.
[39] ByOD (Bring your Own Device): is the authorization to use your own humanl device (smartphone, tablet, laptop) for professional issues.
[40] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4041-ccn-cert-ia-13-19-threats-and-trends-report-executive-summary/file.html.
[41] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
[42] https://www.gartner.com/en/newsroom/press-releases/2019-03-05-gartner-identifies-the-top-seven-security-and-risk-ma
[43] https://www.checkpoint.com/downloads/resources/cyber attack-trends-mid-year-report-2019.pdf
[44] https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html
[45] https://www.kaspersky.com/blog/secure-futures-magazine/2020-cybersecurity-predictions/32068/
[46] CRYPTOMINING is a cyber attack designed to compromise the idle processing of a victim's device and use it to mine cryptocurrency without their consent.
[47] DNS ATTACK is an attack targeting the availability or stability of a network's DNS service.
[48] SANDBOXING is a technology designed to execute untested or unreliable computer programs or codes in isolation to protect services or operating systems.
[49] https://attack.mitre.org/
[50] BOTNET is a network formed by virtually compromised computers (computer robots or bots) that execute tasks autonomously and automatically without the knowledge or consent of their legitimate owners or users.
[51] https://ccdcoe.org/library/publications/guide-to-developing-a-national-cybersecurity-strategy/
[52] https://ccdcoe.org/library/publications/national-cyber-security-strategy-guidelines/
[53] https://ccdcoe.org/library/publications/?focus_area=strategy
[54] https://www.lacnic.net/
[55] https://www.lacnic.net/lacnic33
[56] https://warp.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf
[57] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[58] https://europa.eu/european-union/about-eu/agencies/eurojust_es
[59] ZERO-SUM GAME is a situation in which the gains or losses of one participant are exactly balanced with the losses or gains of the other participants.
[60] VPN (Virtual Private Network) is a technology that enables a secure extension of a private network over the Internet by establishing a virtual point-to-point connection using dedicated connections, encryption, or the combination of both methods.
[61] Paris Call for Trust and Security in Cyberspace (https://pariscall.international/en/)

[62] SCEPVA: Sovereign Cyber Effects Provided Voluntarily by Allies
[63] https://www.iso.org/standard/73906.html
[64] https://www.nist.gov/topics/cybersecurity
[65] https://www.nist.gov/cyberframework
[66] https://www.nist.gov/itl/applied-cybersecurity/nice/about
[67] https://www.ccn-cert.cni.es/guias/indice-de-guias.html
[68] https://www.ccn.cni.es/index.php/es/ccn-cert-menu-es/soluciones-ccn-cert
[69] https://www.ccn.cni.es/index.php/es/menu-formacion-es
[70] https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar.html
[71] https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar/metodologia.html
[72] https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

GUÍA DE
CIBERDEFENSA

ORIENTACIONES PARA EL DISEÑO, PLANEAMIENTO, IMPLANTACIÓN Y DESARROLLO DE UNA CIBERDEFENSA MILITAR