ARI | ARI 26/2013 (Translated from Spanish)
17 September 2013

Real Instituto Elcano

Cyber cells: a tool for national cyber security and cyber defence

Thiber

Theme[1]

Cyber cells are effective tools that enable countries to operate, defend themselves or go on the offensive in a specific area of cyberspace, and they are destined to complement existing cyber security and cyber defence capabilities.

Summary

Except for countries that are pioneers in cyber security and cyber defence such as the US, China and Israel, these days most nations are developing basic cybernetic capabilities, such as information and communications technologies and the organisations and procedures that will make them work when they reach maturity. When this happens it will be necessary to devise the organisations and operational procedures –cyber cells– that allow countries to operate using those previously established capabilities. This paper describes the concept of cyber cells, their functions, tasks and areas of operation, as well as the enablers that will allow them to work. Although it is a matter of a next-generation capability that will complement those which are now being set up, the authors argue that Spain should think about what kind of cyber cells would in fact complement the cyber defence and cyber security capabilities that are being established for use by the military and the national security forces.

Analysis

After several decades shaped by spectacular technological development, a significant lack of attention from politicians and overconfidence among general public about the power, impact, penetration and political, social and economic influence of information and communications technologies (ICT), most governments have begun to take note of both the possibilities and risks that cyberspace entails. Cyber defence and cyber security strategies and organisations abound, and there are many recent studies on them.[2]

[1] The authors are part of the 'cyber cell' working group led by THIBER, *The Cybersecurity Think Tank*, which in turn is part of the Institute of Forensic and Security Sciences at the Autonomous University of Madrid. In alphabetical order, they are: Guillem Colom Piella, who holds a PhD in international security; José Ramón Coz Fernández, PhD in Computer Sciences and BSc in physical sciences; Enrique Fojón Chamorro, computer sciences engineer and member of ISMS Forum Spain; and Adolfo Hernández Lorente, computer sciences engineer and managing director for security at Ecix Group.

[2] Applegate, Scott D. (2012), *Leveraging Cyber Militias as a Force Multiplier in Cyber Operations*, Center for Secure Information Systems, George Mason University, Fairfax, Virginia.

Berman, Ilan (2012), *The Iranian Cyber Threat to the US Homeland*, appearance before the Homeland Security Committee of the House of Representatives, Washington, D.C., 26/IV/2012.

Cabinet Office (2012), *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World*, HMSO, London.

Cyber space was initially considered a global common good for all of humanity, but it is actually far from being neutral, free and independent. In fact, cyber space has been rife with conflict from its very outset and countries such as China, the US, Russia, Israel and Iran are spending huge amounts in terms of human, technical and financial resources to develop cyber forces, with a dual goal: to ensure the security and defence of their specific patches of cyber space while wielding power and influence among their citizens, allies and potential adversaries.

At the same time, as international regulation of the Internet is impossible –and neither is it subject to global governance–, cyber space has seen an increase in the risks associated with the security of advanced countries: a relentless rise in cyber crime, the use of cyber space by terrorist groups for activities involving financing, intelligence gathering, propaganda and recruiting, large-scale cyber espionage between States and/or companies and a spike in crimes against the privacy of Internet users are just some of the challenges that security forces tasked with cyber security must confront.

In the same way and with regard to national defence, the armed forces rely on information and communications technologies to communicate with each other, exercise command and control of operations, obtain and distribute information and intelligence, carry out surveillance and reconnaissance tasks or acquire targets and coordinate fire. So these technologies serve as force multipliers. They optimise the conception, planning and execution of operations and can shape how a conflict evolves and who wins. Therefore, possessing a robust, secure and resilient ICT infrastructure, systematising the dimensions that make up cyber space and integrating them into operational planning or the capability to act in this realm are some of the issues to which the armed forces are paying most attention.

Risk in cyber space

The state of risk in cyberspace is not homogeneous. This is the case both because there are different threat levels for specific national cyberspaces and the cyber security and cyber defence systems and capabilities of different countries are not at all homogeneous. Countries can be broken down into four major groups, depending on the level of implementation and functionality of their national systems of cyber security and cyber defence:

Defence Science Board (2013), *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, US Department of Defense, Washington DC.

Department of Defense (2013), *Defense Budget Priorities and Choices – Fiscal Year 2014*, US Government Printing Office, Washington DC.

Dev Gupta, Keshav, & Jitendra Josh (2012), 'Methodological and Operational Deliberations in Cyber-attack and Cyber-exploitation', *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, nr 11, p. 385-389.

Liles, Samuel, & Marcus Rogers (2012), 'Applying traditional military principles to cyber warfare', Cyber *Conflict (CYCON)*, NATO CCD CoE Publications, Tallin, p. 1-12.

Office of Public Affairs (2010), *US Cyber Command Fact Sheet*, Department of Defense, Washington, DC.

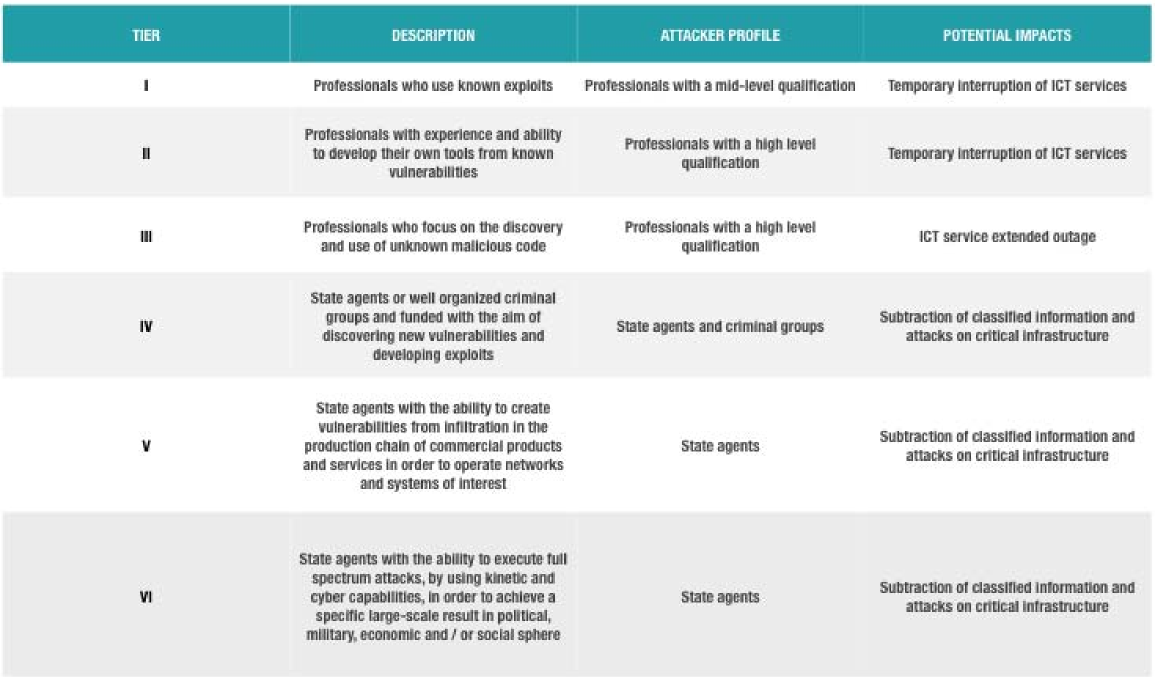
Office of the Secretary of Defense (2013), *Military and Security Developments Involving the People's Republic of China 2013*, US Government Printing Office, Washington DC.

- Group 1, made up of countries with an operational national system of cyber security and cyber defence, formally defined as such and constantly being evaluated, revised and upgraded. Countries in this category would include the US, China and Israel.
- Group 2, made up of countries which are in the formal process of building national systems of cyber security and cyber defence. It would include nations such as Australia, France and Iran.
- Group 3, made up of countries that are in the process –formal or informal– of defining their national cyber security systems. The vast majority of countries would fall into this category, including Spain.
- Group 4, comprising countries which have not yet undertaken a process of defining, be it formally or informally, their national cyber security system.

The US government recently acknowledged that an exponential increase in the volume of resources that its adversaries –particularly China– are earmarking for their cyber forces and the growing technical sophistication of the attacks that these forces carry out are making it tremendously difficult to analyse and research the attacks and therefore to maintain an efficient and effective national defence in cyber space.

Regardless of the origin and nature of the threat it faces, the cyber force of a country should be based on a set of capabilities that allow it to reach a known and controlled state of risk. This state of risk can be attained only by states whose specific cyber spaces feature levels of maturity, resilience and security which, over the short term, are able to withstand TIER I and TIER II level attacks and recover from assaults at the TIER III and IV levels. This is outlined in Figure 1.

Figure 1. Levels of cybernetic threat



TIER	DESCRIPTION	ATTACKER PROFILE	POTENTIAL IMPACTS
I	Professionals who use known exploits	Professionals with a mid-level qualification	Temporary interruption of ICT services
II	Professionals with experience and ability to develop their own tools from known vulnerabilities	Professionals with a high level qualification	Temporary interruption of ICT services
III	Professionals who focus on the discovery and use of unknown malicious code	Professionals with a high level qualification	ICT service extended outage
IV	State agents or well organized criminal groups and funded with the aim of discovering new vulnerabilities and developing exploits	State agents and criminal groups	Subtraction of classified information and attacks on critical infrastructure
V	State agents with the ability to create vulnerabilities from infiltration in the production chain of commercial products and services in order to operate networks and systems of interest	State agents	Subtraction of classified information and attacks on critical infrastructure
VI	State agents with the ability to execute full spectrum attacks, by using kinetic and cyber capabilities, in order to achieve a specific large-scale result in political, military, economic and / or social sphere	State agents	Subtraction of classified information and attacks on critical infrastructure

Traditional capabilities –grouped within the concepts of information security and information assurance– are necessary but not enough in and of themselves to guarantee national cyber security and national cyber defence. So the world's major powers and international organisations such as NATO and EUROPOL are working actively to redefine these capabilities and develop new ones, both to defend and attack.

The increase in the state of risk in cyber space means governments must develop specific capabilities to enhance security and defence in it. One of these is the cyber cell. This is an advanced capability which can complement traditional cyber security and cyber defence capabilities and be used both in a defensive way and to carry out offensive operations in cyber space. Cyber cells are prepared to resolve those operational problems which existing cybernetic means cannot address with sufficient flexibility or effectiveness, and they can be integrated into both police and military forces. With these elements in mind, we will now present the concept of cyber cells and detail how they might be organised and work and what their responsibilities might be.

The cyber cell concept

A cyber cell could be defined as a capability of high functional specialisation and of a dual nature –both defensive and offensive–. Its function is to carry out a task with the goal of guaranteeing the security and defence of a specific area of cyber space. Depending on the operational needs and on the area in which it operates, a cyber cell might be assigned three major functions:

- To carry out specific cybernetic operations or ones in conjunction with other operational dimensions (land, sea, air and space).
- To support the evaluation and improvement of the level of maturity, resilience and security of national, allied and multinational cybernetic capabilities.
- To contribute to experimenting with new operational concepts and cybernetic capabilities.

In the same way, and depending on the function it is carrying out at any given time, a cyber cell can have one of the following four tasks assigned to it: (1) assurance; (2) experimentation; (3) exercises; and (4) operation. In the first three cases the cyber cell will assume the role of a 'red team' under which it will simulate the behaviour of a potential adversary so as to try and exploit the vulnerabilities of the area being evaluated. However, when a cyber cell is in operational mode, it will be able to carry out both defensive and offensive cybernetic activity.

(1) *Assurance:* this will allow analysing the state of maturity, resilience and security of the area in which the cyber cell is operating.
(2) *Experimentation:* here the cyber cell might do a wide variety of things, such as study new operational concepts or evaluate the maturity, resilience and security of new cybernetic capabilities that complement existing ones.

(3) *Exercises:* during exercises the cyber cell must test what it can do. These exercises will be designed and planned with the goal of simulating situations as close as possible to those found in the real world.

(4) *Operation:* when operational needs require it, the cyber cell must engage in defensive or offensive actions, or ones to exploit a given area.

Each of the four tasks assigned to a cyber cell will be executed in a given area of the five outlined as follows:

(1) *Local*, limited to a local ICT system.

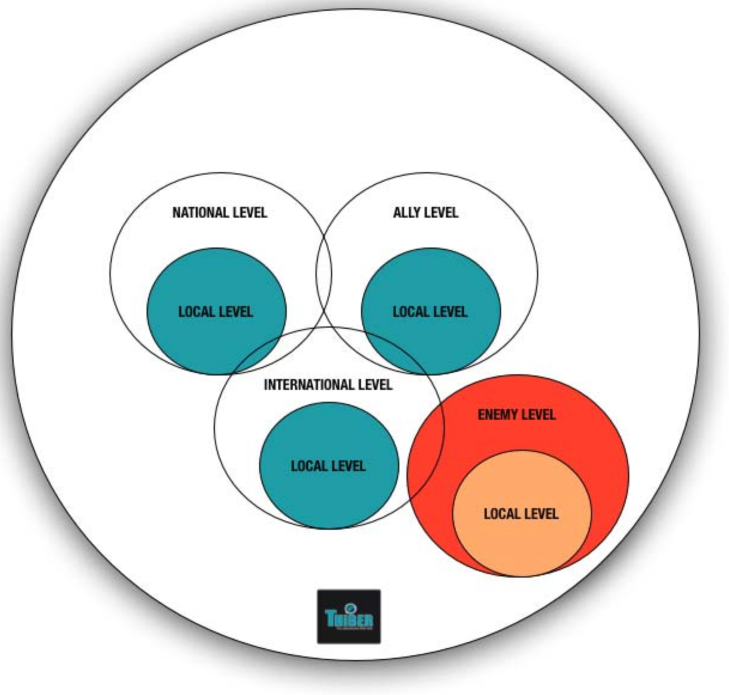
(2) *National*, limited to a local realm or a set of local areas, the command and control of which is exercised by a national body.

(3) *Allied*, limited to a local area or set of local areas, the command and control of which is exercised by an agency of NATO or Europol or bodies belonging to one of their member states.

(4) *Possible adversaries*, limited to a local area or set of local areas, the command and control of which is exercised by organizations belonging to possible adversaries. The nature of the possible adversaries is heterogeneous; they can be States or non-State actors, such as terrorist groups, cyber gangs or so-called *hacktivist* groups.

(5) *Multinational*, defined by a local area or set of local areas, the command and control of which is exercised by a multinational organisation or by a State that belongs to the multinational organisation.

Figure 2. Areas of activity of a cyber cell

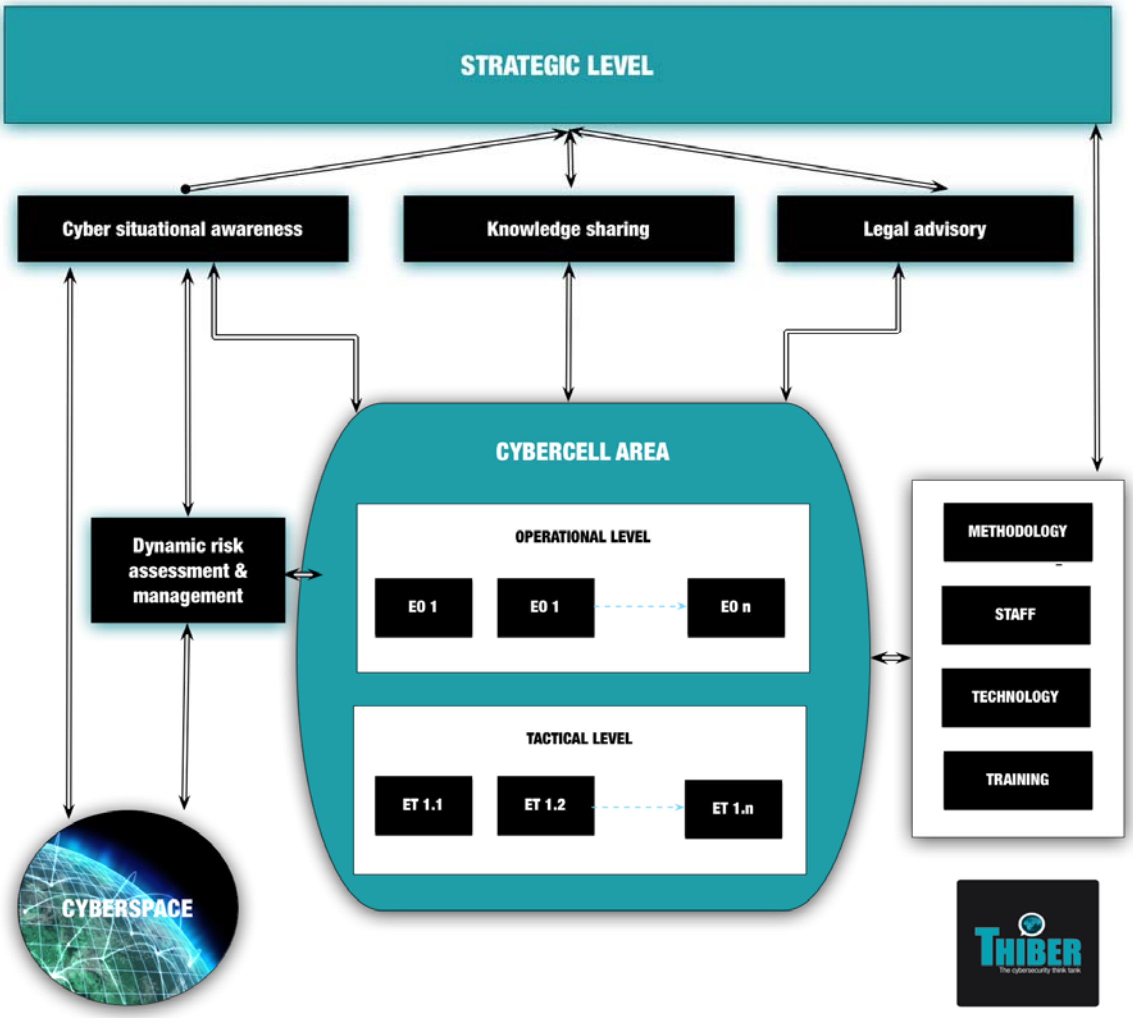


Enablers of cyber cells

Before countries create cyber cells, they must have the right enablers**.** By this we mean those defensive and offensive cybernetic means which have a sufficient level of maturity and are already established in the country and at the disposal of both the security forces and the military. Their existence under the terms described here will make it possible for cyber cells to carry out the tasks assigned to them with some degree of likelihood of success.

These enablers are the following: command and control, organisation, a legislative framework, methodology, knowledge of the cyber situation, risk analysis and management, the sharing of information, technology, staff and constant training**.** Command and control of cyber cells should be exercised at the strategic, operational and tactical levels, and each of these levels will have assigned to it a set of responsibilities and activities so that the cyber cells do their work with guarantees. At the strategic level, the high-level goals, priorities and achievements that the cyber cell must attain as it goes about the task assigned to it will be defined. What is more, from this level the viability and evolution of the cell must be guaranteed, with all necessary human, financial and technological resources provided. At the operational level, all activities related to the assigned task will be authorised and directed, and each will be controlled by an operational team (OT), in such a way that, as the task is undertaken, there will be as many operational teams as there are activities that comprise each task. The make-up of these teams will be determined by the nature of the task. Finally, at the tactical level, the people in charge of each operational team will define the tactical plans related to the activities. In order to do this, they will outline in the greatest detail possible each of the actions that make up an activity, with input from those in charge of the tactical teams assigned to each action (each operational team will be supported by as many tactical teams as there are actions making up the activity).

Figure 3. External and internal contexts of cyber cells



Despite the difficulty inherent in finding those directly responsible for carrying out an act of aggression in cyber space, and the ubiquity, high level of inter-connectivity and cross-border nature of cyber space, the tasks, activities and actions of cyber cells must remain within the bounds of national and international law. In order for the legal framework to serve as an enabler, it must be up to date in terms of regulation of the main elements of cyber warfare and cyber crime, the regulatory frameworks surrounding them and how they are defined as crimes. The legal framework must also regulate the procedural aspects of electronic evidence, criminal justice and international cooperation. Finally, it must be integrated into national and international legislation associated with the prevention of armed conflicts and the exercise of self-defence of sovereignty over national cyber space.

Cyber cells must have a working methodology that features a common language, homogeneous theoretical and technological foundations and procedures that standardise their functioning at the strategic, operational and tactical levels. Furthermore, they must be provided with immediate knowledge of a country's own cyberspace, allied cyber space, multinational cyber space, and that of potential adversaries and any other group that might be of interest, as well as knowledge of the status and availability of the operational capabilities necessary for the planning, leading and management of the activities needed to carry out the cybernetic mission that is assigned. Knowledge of the status of the cybernetic situation will be obtained as a result of combining intelligence and operational activities in cyber space along with those activities carried out in electromagnetic space and any other of the dimensions of the operational environment (land, sea, air and space). So integrating the cybernetic situation with the rest of the capabilities is essential to achieving the goals set out in the task that is assigned. In this way the processes, procedures and capabilities associated with knowing the cyber situation must be developed –always in line with the working methodology that is in place– so that those in charge of the cyber cell attain complete knowledge of the overall cyber situation and can work towards achieving the goals established in the assigned tasks. Furthermore, knowledge of the cyber situation must give the operational leader of the cyber cell real-time visibility of local and national networks, systems and services and of the actions of the potential adversary on the opposing networks, systems and services, as well as the possible impact of these actions on the achieving of operational goals. Knowledge of the cyber situation of the mission and cyber space will also help cyber cells to make decisions if they have the best available information and intelligence and to act if they know the operational effect of their decisions on the mission as a whole.

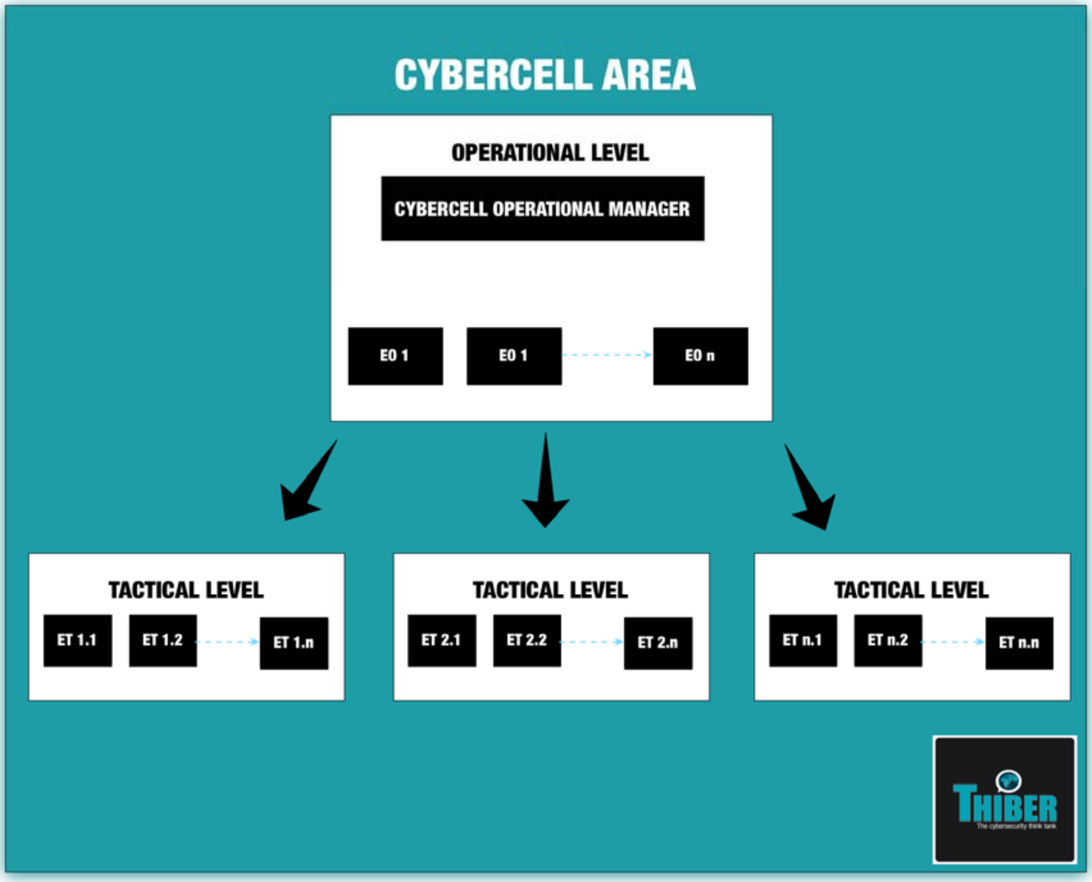
Each task assigned to a cyber cell carries with it a set of risks that will depend on the nature of the task and the realm in which the cell is acting. Therefore, a continuous process of dynamic risk assessment and management in all phases of the task must be developed. In these phases all available information will be collected, analysed and distributed in an appropriate way to the rest of the actors involved in the task. So it will be necessary to devise a set of mechanisms that distribute information in order to have reliable and up to date knowledge of the cybernetic situation, optimise results and improve the maturity, resilience and security of national cyberspace, as well as to manage cybernetic crises.

Technology is the central component of cyberspace. For this reason cyber cells must be equipped with state-of-the-art technological capabilities. They must also be made up of highly qualified and specialised professionals who cover each and every one of the areas of knowledge of the activities and actions that are part of the assigned tasks. It will also be necessary to have a continuous and highly specialised training plan in place depending on each member's specific role in the cyber cell and in accordance with the constant technological transformation of and changing state of risk in cyberspace. Therefore, training will be one of the key elements that will determine the success or failure of cyber cells.

Organising a cyber cell

Figure 4 shows the organisation of a cyber cell as deduced from the command and control structure described in the section on enablers in this paper. The person in charge of the cyber cell's area has responsibility for translating the strategic goals, planning and overseeing the execution of the tasks assigned to the cyber cells, providing knowledge of the cyber situation at all times, directing those in charge of the operational aspects of the mission, and planning training, assessing results, managing risks and enabling the necessary technical and human resources. Reporting to this person are the operational officials. They report to the leader of their area of the cyber cell as to the operational and tactical evolution of the assigned tasks, and have responsibilities that are similar to those of the area operational leaders but at a lower level.

Figure 4. Structure of a cyber cell



Each operational leader of a team will be in charge of carrying out each of the various activities of the cyber cell. This includes reporting to the operational leader of the cyber cell about how the activity assigned is progressing, dividing the activities up into actions, breaking down into as much detail as possible the actions that will be assigned to the tactical teams, planning and overseeing the work of these teams, carrying out a non-stop process of analysis and management of the assigned activities and devising relevant reports on each activity. Finally, each leader of a tactical team will be in charge of carrying out one or more actions, so he will carry out the actions assigned by the person in charge of the operational control team, report to the leader of the operational control team about how the action is progressing, carry out the constant process of analysis and management of the assigned actions and devise relevant reports on each activity.

Conclusions

A cyber cell can be an efficient tool for security forces and the military to improve the security and defence of a given area of cyber space. Cyber cells are composed of operational and tactical teams acting under the control of a strategic cybernetic command and require that from the outset there be a set of mature, traditional cyber security and cyber defence capabilities: a modern ICT infrastructure, a set of cybernetic capabilities and staff that is experienced and used to operating in this kind of setting.

From there on, cyber cells could carry out cybernetic operations both of a defensive and offensive nature, support the assessment and improvement of national, multinational or allied capabilities, allow experimenting with new operational concepts and train people assigned to work in the cell. The implementation of these cells can make a significant improvement to a country's cybernetic defence and offense capability, thus contributing to control of cyberspace and the creation of a modern and effective national cyber force that is completely interoperable with allied cyber forces. In the specific case of Spain, and as is the case with the rest of its allies, efforts must be concentrated on increasing the maturity of the cybernetic capabilities of the security forces and the military over the short and medium term as a step toward the effective establishment of advanced capabilities like cyber cells. However, and again, as its allies already do, Spain should consider establishing them so that capabilities that are under development can become operational as soon as possible.