ACIG APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Shielding the Spanish Cyberspace: An Interview with Spain's National Cryptologic Centre (CCN)

Received: 16.12.2022
Accepted: 10.02.2023
Published: 13.02.2023

Rubén Arcos University Rey Juan Carlos, Madrid, Spain, ORCID: 0000-0002-9665-5874

Abstract

This interview between Rubén Arcos and Spain's National Cryptologic Centre (CCN) was conducted via email on 24 October 2022. CCN is part of Spain's National Intelligence Centre (CNI), and through its national alert and response centre against cyberattacks and cyber threats, CCN-CERT, it contributes to the cybersecurity of Spain. The discussion focuses on Spain's approach to cybersecurity, existing tools for information sharing/management of cyber incidents and tools supporting the production of intelligence on cyber threats. It also deals with current and emerging trends in the cyber domain and developments and activities in the fields of prevention, detection and response. Finally, the interview highlights measures in the March 2022 National Cybersecurity Plan and initiatives against potential cyber-attacks during elections.

Cite this article as:
R. Arcos, „Shielding the Spanish Cyberspace: An Interview with Spain's National Cryptologic Centre (CCN)," ACIG, vol. 2, no. 1, 2023. DOI: 10.5604/01.3001.0016.2484

Corresponding author:
Rubén Arcos, University Rey Juan Carlos, Madrid, Spain;
ORCID: 0000-0002-9665-5874;
Email: ruben.arcos@urjc.es

Spain is very well-ranked in the last edition of the Global Cybersecurity Index of the International Communication Union (ranked 4th together with the Republic of Korea and Singapore) and is within the three top-ranked countries for Europe region[1]. How would you describe the Spanish model or approach to cybersecurity and the reasons that have led to achieving these results?

The Spanish approach is described in the attached document (https://www.ccn.cni.es/index.php/es/menu-ccn-es/aproximacion-espanola-a-la-ciberseguridad), but there are aspects highlighted below in which we believe our approach is leading in the European Union and elsewhere:

- A mandatory National Cybersecurity Framework for the public sector that obliges the application of 7 basic principles, 15 minimum requirements and, depending on the categorisation of the system, up to 73 cybersecurity measures.
  The framework is developed through more than 90 guidelines. It is also flexible in its application to smaller organisations ("PILAR" LEGAL MEASURES);

- An exchange of cyber incidents (more than 15,000 by 2022) across the public sector, which in turn allows for the implicit exchange of IOCs (Indicators of Compromise) and an automatic distribution of cyber intelligence tailored to the needs of the agencies ("PILAR" COOPERATIVE MEASURES);
- Common services for the development of guidelines and standards, as well as training courses;
- Articulation of a national network of SOCs (Security Operations Centers) as a result of previous experience;
- Use of common and interchangeable tools to enforce interoperability in cybersecurity ("PILAR" CAPABILITY DEVELOPMENT).

Which measures, if any, in your opinion would further improve the commitment of Spain to cybersecurity? And how do these excellent outcomes have an impact in deterring attacks from different actors in cyberspace against Spain and its national interests?

In this question we will focus on technical measures, but above all on the smooth exchange of cyber incidents and cyber threats. For this purpose, we use two platforms which, due to their flexibility, allow this exchange between organisations using CCN-CERT as a central exchange point.

- The LUCIA tool enables the exchange of cyber incidents, allowing its adaptation to other ticketing tools used in the organisations, improving the Request Tracker for Incident Response tool (RT-IR) and making it multi-agency with the capacity to federate between the tools used so that the exchange is fluid. Finally, it provides efficiency metrics concerning the resolution of cyber incidents;
- The REYES cyber intelligence tool attempts to tailor this information to the needs of the agencies by providing them with its exposure surface (what the attacker knows about it, vulnerabilities, compromised passwords and other valuable information). Cyber intelligence is also distributed to improve perimeter protection. Finally, the tool provides the necessary information on unknown IPs and domains.

The Royal Decree 421/2004, of March 12th, which regulates the National Cryptologic Centre, establishes the scope of action of CCN as the "security of the Administration's information technology systems that process, store or transmit information in electronic format, that require protection by law, and that include means of encryption" and "the security of information technology systems that process, store or transmit classified information". Considering the current geopolitical situation, how do you assess the probability of the occurrence of a severe attack targeting the systems under the scope of action of CCN?

The probability of a cyber-attack occurring is very difficult to establish. Systems must be prepared in the areas of PREVENTION, DETECTION and RESPONSE.

CCN-CERT promotes actions in these three fields to improve the efficiency of public bodies. In order to do this, the RD 421/2004 is supplemented by the RD 311/2022 of the National Security Framework (which is an update of RD 3/2010). The functions of CCN-CERT are extended here:

- It is the National Government CERT;
- The rapid cyber-attack response enables deployment of early warning systems;
- It provides alerts on vulnerabilities in the technology and within the agencies themselves (due to configuration deficiencies in their systems);
- Deployment of rapid response teams (RRTs) to critical incidents.

[1] Spain top-scores in 3 out of 5 pillars of the framework (legal measures, capacity development and cooperative measures) and has some room for improvement in the pillars of technical measures and organisational measures. See: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Since the beginning of the war in Ukraine, are you aware of incidents in the physical infrastructure (terrestrial cables, submarines) that make cyberspace possible in the Kingdom of Spain or cyberattacks directed at the systems of the general state administration and its public bodies with the purpose of extracting data? What kind of cooperation in this regard have you established with other CSIRTs/CERTs of international partners and allies?

No major incidents directly related to the Ukrainian war have been detected. State-sponsored cyber-espionage actions against sectors of interest to adversaries in the Ukrainian war have been detected.

Theft of sensitive information, intellectual property or state secrets is a common occurrence in our government networks. At least 20 have been detected during the year. No more were detected in 2022 than in previous years.

CCN-CERT has many alliances for the exchange of information, including the European Government CERT (EGC), an informal group of government CERTs in which a lot of valuable information is exchanged.

How does the CCN develop its mission and function in the framework of Spanish foreign policy?

CCN-CERT carries out many training exercises, dissemination of best practices, setting up of SOC/CERT and assistance in the response to critical incidents in many Latin American countries. In addition, the external service is subject to special protection by CCN-CERT.

How many cyber-attacks targeting the public administration systems happen in Spain each year and what percentage of them are related to activity by hostile foreign intelligence services or intelligence activities by non-state actors aiming to exfiltrate classified information or harm national security?

CCN-CERT classifies cyber incidents into five danger levels: LOW, MEDIUM, HIGH, VERY HIGH and CRITICAL. We especially monitor VERY HIGH and CRITICAL incidents.

In 2022, about 55,000 incidents affecting the public sector have been managed. Of these, approximately 70 were recorded as CRITICAL. Of these incidents, 60% are related to cybercrime groups (ransomware) or theft of personal information. The remaining 40% are related to state-sponsored groups (about 30 cyber incidents).

In the latter incidents, if detection is late, it is difficult to determine the volume and type of information extracted, so the impact is difficult to gauge.

What are the main current state-based threats targeting the cybersecurity of Spain? Could you describe some examples of incidents during 2022 involving states actors or APTs?

State-sponsored attacks have focused on the theft of sensitive information from public bodies and companies (in this type of attack, CCN-CERT has the responsibility to act and help the body determine the scope of the attack and remove the threat from its networks).

APT-related incidents are usually classified and it is not possible to report on their scope and typology.

One of the main challenges of hostile activities in the cyber domain is early detection and attribution, could you explain how you gather evidence and assess threat actors involved in cyber-attacks?

CCN is part of the Spanish Intelligence Service (CNI). The attribution is carried out with cyber intelligence units that use information provided by CCN-CERT and other CNI capabilities.

A lot of information about attackers' tactics, techniques and procedures (TTPs) is exchanged to determine attribution with a high degree of certainty.

Have you observed a surge of cyber-attacks during the months preceding the aggression against Ukraine and during the NATO Summit in Madrid?

We did not observe any escalation in cyber-attacks detected during the NATO Summit.

What is the frequency of cyber-attacks targeting critical infrastructure in Spain?

In Spain, critical infrastructure is subdivided into 12 sectors.

CCN-CERT only has visibility on critical infrastructure corresponding to the public sector (government, health, water, transport maritime, rail or underground, food, research facilities).
The detection of cyber-incidents has the same parameters as the general distribution.

What emerging and current trends in the cyber and other domains are deemed to have a significant impact on cybersecurity?

In the last two years the biggest impact on cyber security has been:

- The use of public cloud services as a complement to the services provided by the corporate network;
- The extension of remote work in the organisation's activity. The cybersecurity measures have often not been increased to protect this new working model;
- The use of corporate or personal mobile devices receiving sensitive information from the organisation without adequate protection measures;
- The professionalisation of strike groups.

All these new paradigms make it necessary to work in the fields of:

- PREVENTION: reduce the exposure surface;
- DETECTION: continuous 24 x 7 surveillance;
- RESPONSE: by requiring cybersecurity operations centres that provide this capability horizontally to a variety of agencies.

Could you explain how CCN-CERT conducts early warning procedures and how the Early Warning System (SAT) operates?

The early warning systems operated by CCN-CERT began to be developed in 2008. They are deployed on a voluntary basis in agencies. They are rule-based systems that provide detection capabilities for known cyber-attacks. The detection rules are updated daily and use both their own and external sources (commercial feeds).

The logs generated can be exploited by the organisation or alerts can be received directly from CCN-CERT.

And they cover the following fields:

- SAT SARA. It provides detection capacity to the Governmental Network (RED SARA) that interconnects the central administration, regional governments and local entities. An aggregation of logs from the perimeter devices of the connection areas of the different bodies that are connected is carried out. There are 50 sensors;
- SAT INTERNET. Intrusion detection system in the Internet traffic of the organisations. It includes various technologies to fine-tune this detection capability. There are more than 320 sensors available;
- SAT ICS. It is a detection system for industrial networks or corporate networks that include many devices using industrial protocols (e.g., hospitals). It performs asset survey and dissection of industrial protocols. More than 50 sensors are available.

These systems can detect known attacks and enable rapid defence against new cyber-attacks or new malware samples. All detection is based on the analysis of network traffic.

The CCN website is remarkable for the information and public reports shared. Could you explain what other kind of information products (non-public) you produce?

Regarding the public reports, in addition to the CCN-STIC guides we can point out the threat reports (IA), malicious code analysis reports (ID) and best practice reports (BP). Most of these reports are available on the website.

Furthermore, CCN-CERT prepares Technical (IT) reports that are associated with the investigation of cyber-incidents or the performance of audits. These reports are sent to the body or bodies concerned. In 2022, around 100 reports were produced.

What measures of the National Cybersecurity Plan, approved by the Council of Ministers on March 29, 2022, did you consider most relevant and are having or have the potential to make a greater impact?

The measures that will have the greatest impact will be those related to:

- Boosting the implementation of the ENS;
- Development of Cybersecurity Operations Centres and their integration into the National SOC Network;
- Development of active cyber-defence measures to take the initiative against cyber-attackers;
- Development of training/awareness raising systems to improve their level.

These actions should be accompanied by corresponding metrics.

How does CCN-CERT work in the prevention, detection, and neutralisation of cyberthreats and operations in cyberspace by threat actors?

Cyber operations on cyberthreats are offensive activities that are not the responsibility of CCN-CERT.

Does the CCN and/or CCN-CERT have a role against foreign information manipulations and interference within cyberspace? Do you monitor hostile narratives and disinformation from foreign state actors targeting Spain?

The disinformation activities are not the responsibility of CCN-CERT.

What capabilities or measures has Spain developed against emerging threats like Deepfakes or synthetic content for cyber and influence operations by foreign and criminal actors?

This activity is not the responsibility of CCN-CERT.

From the perspective of training curricula, what gaps/needs in competences or skills have you identified, or do you consider to be very relevant for strengthening cybersecurity?

We need very specific technical skills in system audits, investigation of cyber incidents (in particular, reverse engineering, mobile phone analysis and mass LOG analysis).

What relative percentage of cyber incidents in Spain originate from domestic *vs* foreign threat actors?

Most cyber incidents (80%) originate from external actors.

Do you conduct simulations or wargames with stakeholders in the scope of action of CCN to assess potential cyber or crisis scenarios or test gaps and needs in capabilities?

We conduct cyber exercises focused on crisis management of cyber-attacks by state-sponsored actors (APTs) and cybercrime groups (ransomware).

They are based on the CCN-CERT's experience in dealing with this type of attack.

How do you foresee the future of cybersecurity? What technologies have a greater disruptive potential?

Artificial Intelligence based on detected traffic will allow analysts to focus on tailored cyber-attacks. All of our systems must migrate to AI-based technologies.

This discipline should be complemented by threat-hunting activities based on the experience of analysts.

On a scale of 0 to 10, how do you assess the state of cybersecurity culture in Spain? Do you think the autonomous communities and local administration have a high level of commitment to cybersecurity?

Awareness has increased considerably in Autonomous Communities and Local Government following the ransomware attacks we have undergone. We estimate that we have moved to a level of at least 8. The role of cybersecurity managers has been greatly strengthened.

What specific measures could promote and bootstrap SME's cybersecurity or their cyber hygiene practices?

In Spain we have an adaptation of the National Security Framework for small local administrations with 35 adapted measures that allow for adequate cybersecurity. This system could be adapted to small and medium-sized enterprises also.

2023 will be an election year in Spain – what initiatives has Spain developed against election interference and for countering potential malicious activities in the Spanish civilian cyberspace in this context?

CCN-CERT carries out a deployment during elections that supports the Ministry of Home Affairs or the corresponding Autonomous Community to protect the electoral system from cyber-attacks.

Activities include:

- Audits of all systems involved, identifying and prioritising the vulnerabilities to be addressed;
- Cyber-surveillance campaign to identify possible actors that could carry out attacks on deployed systems;
- Continuous surveillance during Election Day until the presentation of results to the public.

Other comments or aspects that you consider relevant from the CCN's point of view regarding the Kingdom of Spain's cyberspace and cybersecurity?

The protection of Spanish cyberspace is the CCN's fundamental objective. To achieve this, it is necessary to count on all the agents that contribute to this activity and to form a SINGLE CYBER-SHIELD as the motto of our XVI Jornadas STIC CCN-CERT, the largest cybersecurity event organised in Spain and held just a few weeks ago.