Public-Private Partnership: The Missing Factor in the Resilience Equation - The French Experience on CIIP

by Danilo D'Elia*

Introduction

For many years, information security has been the exclusive domain of a closed community of people from military, academics and IT companies. The information revolution in the 90s radically changed the scale and the nature of the issue. With the massive penetration of digital information and communication technology (ICT) in all advanced economies, people and engineered machines are now part of the same global environment made of information: the *infosphere*. Moreover, due to the deregulation process of many public sectors in the 80s and the globalization of 90s, the private sector now owns the majority of critical infrastructures, including information networks, and is at the core of the ICT expertise. Therefore, this revolution brings the problem of Critical Information Infrastructure Protection (CIIP) beyond traditional national defense circles and the terms of the political debate around CIIP are now focusing on a main point: the cooperation between public authorities and the private sector is needed to enhance resilience, but its implementation is hard to achieve.

A Schizophrenic State No Longer at the Centre of the Security Realm

While cooperation is needed and obvious for both the public and private actors, determining how to organize the relationship presents a complex problem due to a conjunction of factors acting on several layers.

First of all, behind the oversimplified categories of public and private, various actors with conflicting representation and interests interface with each other. On the private side the players include infrastructure operators, maintenance firms, incident command system (ICS) providers and security companies. With the emergence of the CIIP issue, a main divergence appeared: the different culture between IT security (protection against intentional damages) and safety of operational technology, OT (protection against accidental events). Historically, confidentiality is not the main consideration in OT systems, and availability and integrity are by far the dominant concerns. On the other hand, OT systems frequently have little or no intrinsic security behavior. Although Stuxnet and recent events have encouraged ICS vendors to improve the security of their systems, some are only moving slowly, and many legacy systems will continue in service for many years with little or no built-in security due to the long life cycles of OT systems when compared to IT systems.

On the public side also, the presence of various players generates a fragmentation of the role of public sector: national intelligence, law enforcement, defense, emergency management, health services and first responders. Thus, four major challenge are undermining the implementation of PPP: unclear delineation of roles and responsibilities of players, lack of trust between partners, different languages (technological vs. bureaucratic), diverging interests (security vs. corporate benefits), and misplaced expectations (national security vs. multinational availability).[2]

Moreover, protecting against cyber threats has led to a contradictory practice and has revealed the schizophrenic conduct of national security authorities. In many countries,

(Continued on Page 11)

[1] This publication is a short version of the article presented at the CRITIS Conference 2014: the full-length article is forthcoming for Springer edition 2015.

[2] Myriam Dunn Cavelty and Manuel Suter, "The Art of CIIP Strategy, Taking Stock of Content and Processes," in *Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense*, ed. Javier Lopez, Roberto Setola, Stephen Wolthusen (New York: Springer, 2012), 15-38.

(Continued from Page 10)

intelligence services and defense agencies are developing offensive capabilities for security interests. To achieve that, they exploit vulnerabilities in current operating systems and hardware or contribute to new vulnerabilities in widespread encryption systems. This situation makes the risk assessment more complex: backdoors could be identified and exploited by malicious actors and thus reduce the resilience of the entire system.

Therefore the dialogue is inherently difficult. In accordance with the development of a comprehensive risk analysis, we argue time has come to define PPP through a new ethos. As do the technical security solutions and the insurance policies, PPP should be approached as a variable of the resilience equation and a risk mitigating factor.

The French Feedback Loop Process and Its Limits

In accordance with the objective to become a world power in cyber defense, France has launched numerous initiatives to ensure CIIP. Table 1 summarizes the main moves and highlights the global impact on cyber risk. If viewed broadly, these initiatives enable the move

FRENCH CYBER RESILIENCE EQUATION			
Domain	*Initiative*	*Description*	*Influencing*
Security standard	Working group on ICS security	Working group established by ANSSI (national authority on cyber security) and bringing together all the stakeholders involved in CIIP. Focusing on : security standard, risk management and trusted solutions.	Countermeasures Vulnerability Impacts
	Military Programme Act 2014-2019 article 22	Security Standards and legal measures to be imposed to CIs: mandatory cartography of the critical information systems; mandatory and regular audits of information systems and networks; mandatory declaration of cyber incidents; implementation of certified sensors.	Countermeasures Threats Impacts
Education & Training	French Centre of excellence for fight against cyber crime	The Centre is a PPP focusing on training and involving four companies (CEIS, Microsoft, Orange, Thales) three universities and the Gendarmerie.	Impacts Vulnerability
	Cyberdefence Cluster	Private company from telecom sector as well as from security and defense will jointly cooperate with the main research laboratories and MoD agencies in promoting innovation and training the future experts.	Countermeasures Vulnerability
	Chaire Thales Cyber defense	Research Program founded by private sector (Thales&Sogeti) in cooperation with the MoD. Focusing on cyber defense and developing courses and training for military.	Vulnerability
Awareness	Network of cyberdefence reservists	Network of reservist made up of about 100 citizens helping in raising awareness, debating and suggesting, organising and establishing events that contribute to making cyberdefence a national priority.	Vulnerability
	Awareness campaign led by DCRI	In 2012 the Central Directorate of Interior Intelligence (DCRI-Ministry of the Interior) lunched an awareness campaign on cyber risk targeting CIs employees and managers.	Vulnerability
	Chaire Airbus Cyber stategy	Research centre founded by Airbus Foundation in cooperation with and the Institute of Advanced Studies in National Defence . Focusing on geopolitics of cyber security and aiming to create a national community of researchers on cyber security issues.	Vulnerability
Trusted solutions	Industrial Cyber Plan	ANSSI is in charge to release a road map in order to boost the national cyber industrial base. The aim is to develop a sovereign industrial ecosystem and to develop a strategy in cooperation with the private sector.	Countermeasures
Information Sharing	Club des Directeurs de Sécurité des Entreprises	French Club of Security Managers is a non-profit organisation allowing CIOs, risk manager to meet, work and exchange information.	Threats
	CERT FR	French government CSIRT. As such, CERT-FR is the point of contact for all computer-related security incidents regarding France.	Vulnerability
Exercise	Piranet	Part of a series of national level crisis management exercises organised by the SGDSN. Tha aim is to test the crisis prevention and management plans. More than 500 public & private participants.	Impacts

(Continued on Page 12)

(Continued from Page 11)

from a supposed high-level of risk (A) to a low-level of risk (B) and thus reducing the severity. In France the CIIP is historically organized as a cross-ministerial issue and the operators, according to the legal umbrella called *SAIV Framework (Secteurs d'activité d'importance vitale)*, bear the financial and operational burden. Due to space constraints, a complete analysis of moves cannot be covered at much length, thus we selected a critical initiative on the field of the PPP: the SCADA working group.

Bridging the Gap between National Security and Operational Life of CIs

In 2009, a specialized agency in charge of the defense against cyber threat (French Network and Information Security Agency-ANSSI) was established and the strengthening of CIIP was defined as a major objective of cyber security strategy. Nevertheless, over the last years, several major attacks were disclosed and thus the 2013 White Paper on Defense and National Security defined cybersecurity as an element of national sovereignty and the government imposed additional constraints to CIs.[3]

The ongoing evolution of the SAIV framework shows that the traditional role of public authorities as rulemaker is still essential. On the other hand, the CIIP has to be thought as an adaptive process: standards are continually being established and updated, thus regulation needs to be reviewed over time to try to fit with new risks. However, due to the features of ICT environment, evolving much faster than the standard setting process, regulation could be only a stopgap and is not a silver bullet solution.

Here the PPPs play their crucial role: despite the enforcement of new standards, the public authorities defined the situation as unsatisfactory. Thus the second step of French strategy was the identification of the missing bricks in order to better mitigate the risk.

Particularly ICS security was identified as a main concern, thus ANSSI conducted a series of interviews in 2010 with CI operators, security suppliers and ICS vendors. The goal was to draw a shared understanding of the limits of the current security infrastructure, where best practices were to be found and the need of future requirements. In that way, the national authorities aim at establishing new standards and in parallel working with the industry to offer tailored solution for CIs.

However, the differences of language and culture emerged again.[4] In 2011, ANSSI was aware of that and created a department fully dedicated to foster cooperation with CIs. In addition, a permanent exchange platform (SCADA Working Group) was established with the main stakeholders from government (ANSSI and MoD) and industry (SCADA providers, national CIs and security suppliers) to establish best practices on supply chain risk management.

In parallel, a twofold initiative has been launched. The certification process, led by ANSSI, for the rating audit companies as independent evaluators states how well CIs have implemented the new framework. In addition, the standardization process refers also to trusted solutions and vendors. As showed by the Snowden affairs, a strong domestic ICT industrial base is a strategic advantage in cyber conflicts. The knowledge of software or hardware vulnerabilities could be exploited for both espionage and sabotage. ANSSI is promoting and leading the development of trusted suppliers by the accreditation process through the on-the-field expertise acquired through incident response and recovery.

These moves stress how cyber risk depends on so many variables that public and private players can impact only through a coordinated approach. The first important achievement is the mutual understanding of various interests and thus the convergence of opinions in adopting minimum security standards. In doing that, the SCADA WG reduces the gap between the

(Continued on Page 13)

[3] Military Programme Act 2014-2019 article 22, available at http://www.senat.fr/leg/pjl13-196.html. The measures include: mandatory cartography of the critical information systems, mandatory audits of information systems and networks by certified third parties; mandatory declaration of cyber incidents; implementation of certified sensors; more power to State authorities in order to take exceptional measures in case of a serious crisis.

[4] Stephane Meynet and Mathieu Feuillet, "SCADA/ICS Security ANSSI Working Group," Presentation made at the CESAR Conference 2013 (20 November 2013).

(Continued from Page 12)

government's lack of a technological path and the CIs' lack of a security path and contributes to better assess future needs for CIs. The outcomes of these initiatives could directly impact the risk factors, elaborating the secure design of new ICS leads to reduce the technical vulnerabilities. On the other hand, the implementation of trusted products, such as the detection sensors, generates more countermeasures and a broader view of frequency and gravity of cyber attacks.

In that sense, the process launched in 2010 is a first important step to organize the public-private dialogue. However, a more in-depth analysis reveals important tensions that might be potentially damaging the implementation of the dialogue. On the private side, increasing critics have been heard condemning the regulatory-based approach without taking the market drivers into account. The primary interest of CI operators is to employ solutions broadly adequate for multinational plants. For security suppliers their concern is more for developing solutions able to be sold on the international market. Here is where corporate interests clash with national security and highlight the need of more international cooperation. Since CIIP is defined as matter of national sovereignty, public powers are imposing new constraints to CIs and influencing the development of national technologies which should fulfill national standards. The consequences, such as limitation of foreign investment and increasing cost to implement a multitude of national standards, are relevant for the private sector.

In conclusion, these dynamics underscore the need to find the balance between national sovereignty and global business interests. That leads to the question of the right scale of international cooperation: how does one define a good partner? Is the European Union's the most appropriate level, or it would be more valuable to establish a trusted group of partners on the basis of mutual acceptance of national standards? The issue is complex, and the debate is still ongoing in Europe.

Gaming the Future: Public-Private Debate and 3PStrategy

The implementation of CIP is never going to be simple, but the French case outlines several important insights. Due to the complexity of the resilience issue, the State needs to make a preliminary capability assessment (which capabilities are needed to be jointly developed with the private sector?), then various and interdependent initiatives should be established with the private sector. PPP and regulation, thus, are complementary measures of infrastructure resilience. On the one hand, the government's responsibility is to build the appropriate and continuously-updated framework, both at national and international levels. On the other hand, PPPs operate to address the missing bricks that need a cooperative approach: training, situational awareness of attacks, technical solutions, etc. As demonstrated by the evolution undertaken by ANSSI in 2009-2013, dealing with CI resilience means being adaptive: being the policeman (conducting the inspection), the conventional rulemaker (helping CIs understand the measures to be implemented) or the facilitator (to develop the technical solution). Given that, the State takes on other important roles in enhancing the cyber resilience.

First of all, the debate on the balance between law enforcement, security and offensive capabilities must be open. Keeping secret vulnerabilities or cracking encryption standards means increasing technical vulnerabilities for everyone. In that way, the State schizophrenia (promoting and implementing defenses while actively attacking) is no longer sustainable with the concept of resilience. However, the schizophrenia is also on the citizen's side: we accept that the State needs pre-emptive intelligence in order to anticipate the major threats to CIs. This situation pushes States to openly explain their activities—without revealing security recipes—to the citizens.[5]

In addition, public power should establish a strategy of PPPs that will evolve as the risk evolves. The real question is not about what exactly the role of government and private sector is, but rather how the different pieces of public-private cooperation fit together in order to mitigate the risk. CIIP is neither a state nor a solution but a continuous process

(Continued on Page 14)

[5] David Omand, Securing the State, (London: Hurst, 2010); Bruce Schneier, "A Fraying of the Public/Private Surveillance Partnership," Schneier on Security, last modified November 2013, https://www.schneier.com/blog/archives/2013/11/a_fraying_of_th.html.

(Continued from Page 13)

based on dialogue and demanding different levels of intervention from public and private sector. Therefore, a large and trusted spectrum of PPPs can act directly as a mitigation tool able to improve the national resilience.

With this new ethos of PPP, the State and private sector can play an increasing role in reducing the overall impact of the cyber risk and improve the ability of organizations to defend themselves against cyber threats. At this stage more detailed studies should follow on specific cases, and since the CIIP topic includes transnational issues, further research on regional and international level of PPP should be encouraged.

Acknowledgements

This work is funded by *Airbus Defence and Space-CyberSecurity* and supported by the *Chaire Castex de Cyberstratégie*. Any opinions expressed in this publication are those of the author and do not necessarily reflect the views of Airbus Group.

**Danilo D'Elia is a Ph.D. candidate in Geopolitics at the University of Paris VIII Saint-Denis and research associate at Chaire Castex de Cyberstrategie (Paris). His research focuses on the dynamics of the implementation of the French strategy of cyber security.* ❖

CIP/HS is involved with a three year research study for the Department of Homeland Security looking at Improving the Effectiveness of Cybersecurity Incident Response Teams (CSIRTs). If you are a member of a CSIRT team or if you are involved in your organization's cybersecurity management or operations, we would like you to consider taking the attached survey. A link to the survey can be found here: https://www.surveymonkey.com/s/MHVXQTQ.

The survey should take 10 to 15 minutes to complete. The data collected in this study will be confidential and no individual or organization can be identified. A summary of the research results will be presented at future cybersecurity conferences and published in a future edition of the CIP Report.

Any questions on this survey or the DHS research study should be directed to me 703-993-4720 or via email at mtroutma@gmu.edu