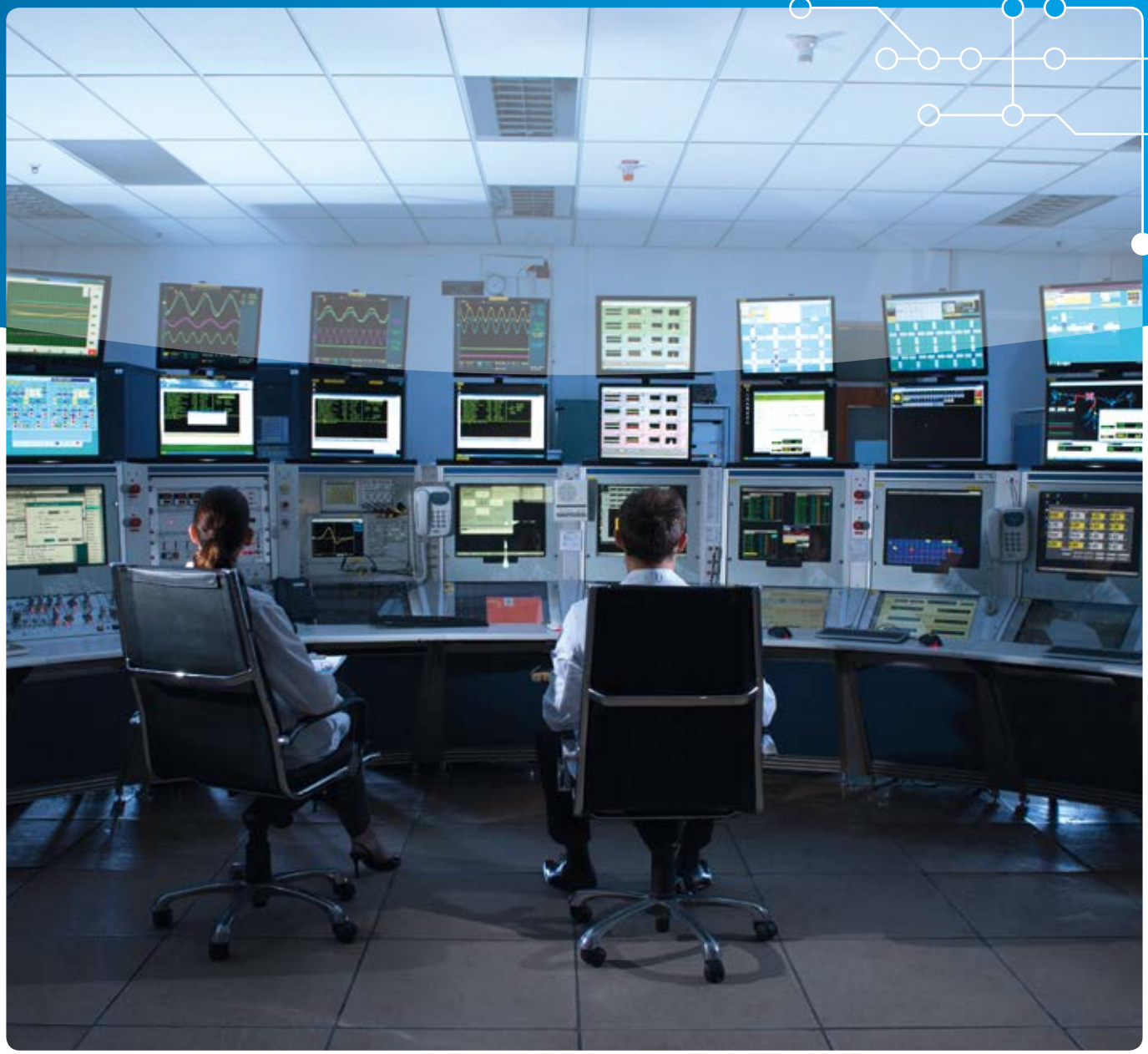
Securing Critical Infrastructures in the Netherlands

Towards a National Testbed



The Hague Security Delta

Securing Critical Infrastructures in the Netherlands

Towards a National Testbed

The Hague Security Delta

Abstract

This report presents the rationale for developing a holistic approach to securing Critical Infrastructures (CIs) in the Netherlands through, among others, the use of a multi-sector testbed. Industrial processes are becoming progressively digitized, and society is increasingly adopting digital technologies. The security side of this technological advancement, however, has taken a back seat. Industrial Control Systems (ICS) in our CI may be prone to cyber attacks such as hacking, social engineering, overloading, malware, exploits, physical attacks, and electromagnetic attacks.

These attacks affect the operations of public and private sector organizations alike and can also have large-scale societal consequences as disruption of CI services were identified in various national risk assessment scenarios. Through amulti-sector approach, CI operators, owners, and manufacturers can benefit from information sharing and exchange of best practices. Given the high number of financial losses, the large number of leaked user information, and the potential societal damage, it is now the appropriate time to seek a more holistic and comprehensive approach to the issue of cybersecurity. In addition to addressing the security concerns, this approach could positively influence the economic performance and position of the Netherlands.

Table of Content

This digitization has occurred over the last two decades and has taken control over the creation, transfer, and storage of our industrial processes at the core of our Critical Infrastructures.

1 – Accomplishing the Digital Age in Industry

We have moved into a digital world where services and goods are produced, delivered and sustained by processes and machines that have become digital. This development has taken place in all aspects of modern society, from the power that is produced for homes and industry, food that is produced and processed before it hits the supermarkets, our phone and internet communication, our banking system, international trade, and diplomacy. This digitization has occurred over the last two decades and has taken control over the creation, transfer, and storage of our industrial processes at the core of our Critical Infrastructures (CIs).

An industrial system is considered digitized when its operation is controlled and calibrated by a computer. These industrial processes are digitized through the use of Industrial Control Systems (ICS) such as Supervisory Control and Data Acquisition systems (SCADA), Distributed Control Systems (DCS), and Programmable Logic Controllers (PLC). These are systems that control multiple processes of repetitive and continuous operations such as the rotation of a centrifuge. These systems run in an operating environment that is programmed to adjust the speed, temperature, precision, rotation of the operational processes depending on their intended function. Their makeup is often very diverse and complex, containing equipment from a wide variety of vendors, designed for idiosyncratic processes, and with legacy components sometimes dating back several decades. These operational environments have increasingly moved from a standalone setting to a networked environment.

This change provides operators critical information about the system performance, simplifying and making production more efficient and effective and allowing remote access to optimize their functionality.

Depending on the industry, the computers in these operational environments may be linked to external monitoring centers that process the sensory data. These centers aim to identify automatically problems in the machinery in real-time before the problem becomes severe or causes an outage. Such systems are now implemented in food production, power plants, bridges, hydroelectric dams, telecom towers, and satellite communication and provide considerable economic opportunities to reduce cost and develop new, tailor-made services and are often in operation 24/7. Many of these industrial processes occur in our CIs.

Dataplace Alblasserdam

Critical Infrastructures are the clockwork that makes modern society tick.

2 – What are Critical Infrastructures?

Critical Infrastructures (CIs) are the clockwork that makes modern society tick. CIs are the sectors defined to be of most importance for the functioning of society. According to the European Commission's definitions, CI are 'those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments.'[1]

In the Netherlands, a revision of critical infrastructure sectors and services was presented in May 2015.[2] The revision resulted in an updated, comprehensive list of sectors, divided over two categories. Category A has been defined as infra-structures that reach a certain threshold for one of four impact criteria: economic impact (damage or drop in GDP), physical impact (casualties), societal impact (survival or emotional problems), or cascading effects. For category B, lower thresholds have been applied to the first three criteria.[3]

Category A

- National transportation and distribution of electricity
- Natural gas production
- Oil supplies
- Storage, production, or processing of nuclear materials
- Drinking water supplies
- Water management

Category B

- Regional distribution of electricity and gas
- Flight and airplane management
- Maritime and inland shipping management
- Large scale storage, production, or processing of petrochemical resources
- Financial sector (banking services, electronic transfers between banks and between banks and the public)
- Communication with and between emergency services
- Police mobilization
- Government services that depend on reliable, available digital information and data systems

'There is a 10 to 20 percent chance of a major breakdown of CI within the next decade, potentially costing 250 billion dollars.' Source: World Economic Forums 2008 Global Risks report.

3 – Threats to Industrial Processes in our CI

Although the digitization of industrial processes allows for convenience and provides many economic benefits both to operators and end users, it also opens the door for vulnerabilities and risk.

ICS have been incrementally upgraded over the past years and are often composed of numerous elements that originate from different vendors and have been patched in various stages of their implementation.[4] These digital processes are more vulnerable than their analog predecessors. This is because they are harder to track and monitor, can be easily impacted relatively easy without a significant investment, and the skills required to inflict damage are publicly available. According to World Economic Forums 2008 Global Risks report, the offline costs of cyber attacks were estimated to average €4.9 million a day and peak at €7.6 million a day for the Energy Sector. The same report states that there is a 10 to 20 percent chance of a major breakdown of CI within the next decade, potentially costing 250 billion dollars. The 2015 iteration of the Global Risks report estimates that the impact and probability of such a breakdown are increasingly more likely.

Digital ICS processes present companies with a vast number of risk factors to take into consideration, ranging from the disruption of services, degradation of performance to the destruction of machinery and goods. These can be triggered by unintended events or can be orchestrated through cyber attacks or physical engagement. While the US and the UK have started to regulate the players within the CI sector (through standards and requirements), most EU countries are still looking at private CI companies to take care of their own policies towards cybersecurity.

Cyber attacks consist of different activities, such as making use of malware, social engineering, overloading processes, hardware and software weaknesses, physical attacks, and electromagnetic attacks. They are performed to sabotage or steal information from a particular computer system or render it dysfunctional. Examples of attacks are Distributed Denial of Service (DDoS) attacks, Trojans, Structured Query Language (SQL) injections, Bot-Network attacks and Zero-Day exploits.[5] These sorts of attacks can be orchestrated by hackers, cyber criminals, hacktivists, competitors, other nation states, and amateurs. Since the skills required to program and carry out these attacks have become decentralized and more accessible, attackers can pick up these skills quite quickly and can make them available to others in the form of *script kiddy tools*.[6] The range of cyber-attacks can vary from simple attacks that require a few clicks, to very complex ones that require thousands of coding hours, and capital investments in logistics and acquiring Zero-days. The consequences of these attacks can also range from information leakages, irregular machine activity, to more severe consequences such as machinery coming to self-destruct and cause real damage.

The risk depends on the intent and sophistication of the attacker. Cyber attacks can be classified as acts of illegal intrusion, theft, excessive protest, sabotage, theft, espionage, and in some instances even as acts of war.

Acts of cyber-sabotage require extensive knowledge of the targeted system, tailored computer code and are usually driven by a political or economic purpose. The most notorious act of sabotage today is the case of the Stuxnet virus.[7] The Stuxnet virus is claimed to be the first of many highly sophisticated pieces of computer code intended to disrupt operations in a nuclear enrichment facility in Natanz, Iran. Through a sophisticated peer-to-peer spreading, the computer code targeted the Step-7 software in a PLC that controlled the ultracentrifuges processing uranium. The code caused the ultracentrifuges to increase and decrease rotation in specific intervals. Consequently, this caused the aluminum casing of the ultracentrifuges to expand and thus collide, damaging over 100 centrifuges and causing the yield of the process to decrease.[8] Recently, a private sector example of cyber sabotage was seen in Germany when an unmanned steel mill was hacked. This was done by manipulating and disrupting the PLCs to such an extent that the blast furnace did not properly shut down and thus resulted in unspecified amounts of damage.[9]

In the Netherlands, we saw examples of disruption in 2012 when the financial sector was hampered due to a series of DDoS attacks. These attacks ultimately cost the companies involved millions of euros in interrupted services, replacement of hardware, work-hours in mitigating the attack and were liable for inconveniences caused to their customers.[10]

In addition to these consequences occurring during the attack, these companies also face damage to their reputation as their ability to protect and mitigate cyber-attacks comes into question and may affect public trust in the company. According to Kaspersky Lab, a recent series of cyber attacks by the *Carbanak cybergang* targeted about 100 banks and accumulated around $1 billion, showing just how serious cyber threats are to the financial sector.

Above all, the impact of the risk is exacerbated by the inter-linkages across all these systems. Virtually all companies currently use ICS for the production of services we deem critical. These systems have become nodes in the extensive network of CI, creating cross-sector and transnational dependencies. Diverse critical sectors heavily rely on each other for the production of (critical) services and goods. The Food sector relies on the Transport Sector to deliver goods, the Banking sector relies on the Telecom Sector to authenticate transactions, and almost all sectors will rely on the Surface Water and Energy sectors for daily operations in the Netherlands.

CI systems are also interdependent of other CI across national borders. In 2006, a cruise ship called *the Norwegian Pearl* traveled through the Ems River to the North Sea. That required a high voltage power line to be switched off temporarily and caused an unexpected trip of the Landesbergen Weherendorf electric transmission line. The result was a black out within 80 seconds across Germany, France, Italy, and parts of Spain, Portugal, the Netherlands, Belgium, Austria, Switzerland, Hungary and cascaded as far as Morocco.[11]
The power outage affected 15 million users and lasted between 30 minutes up to over 15 hours. This mishap very clearly illustrates the fragility and cross-border nature of some of our CI. The truth behind these examples is that our CIs are only becoming more interdependent and interconnected as services become digitized.

The creation of a multi-sector testbed will bring economic benefits in terms of prevention of data loss, in the prevention of disruptions, in saving costs by sharing the expenses, and in attracting new CI operators and manufacturers to the Netherlands.

4 – Benefits for the Netherlands

Thus, the impact of the disruption of such services can be felt at all societal levels. The societal implications of an outage of a particular CI can affect all people who have gone without the service, and these effects will spill over and also affect the political levels. At this top level, the national government will ultimately be held responsible and accountable for the mishap occurring from mainly privately own CI services and goods, making the private sector risk a political and governmental issue.

The Hague is becoming a European hub for cybersecurity

Economic: The creation of a multi-sector testbed will bring economic benefits in terms of prevention of data loss (mainly in the form of intellectual property), in the prevention of disruptions, in saving costs by sharing the expenses, and in attracting new CI operators and manufacturers to the Netherlands.

Better security: The creation of a National CI testbed would be a step forward towards improving national and European security. Through information sharing, agreeing on best practices and through training, CI components would be tested to industry standards that would be shared by all CI sectors. This cooperation would benefit the private sector, government, and the end user.

The Netherlands as a beacon for cybersecurity: The Netherlands, and more precisely The Hague, is becoming a European hub for cybersecurity. Having NATO NCI Agency, the European Cyber Crime Center (EC3) and Eurojust all in The Hague creates a niche environment for tackling cyber-security issues. The creation of a multi-sector testbed to secure IT and OT would be highly complementary.

Cooperation in this domain requires efforts from both the companies in the private sector that own, operate and manufacture the CI, and the policy makers.

5 – A Holistic Approach to the Problem

Given the interdependencies and scale of the possible disruptions, addressing the risks of our CI requires a holistic approach. Cooperation in this domain requires efforts from both the companies in the private sector that own, operate and manufacture the CI, and the policy makers that regulate business practices, set security standards for public goods, and are responsible for maintaining public order, safety, and security.

A comprehensive approach needs to tackle the issue of improving the security of our CI, legislation and regulation need to be comprehensive, and CI standards and trans-national cooperation have to be addressed at the international level.

1 **Improving the security of our CI** at strategic, policy, and technical levels, which can be achieved through a multi-sector testbed among others? The creation of a national testbed infrastructure would allow for different CI owners, operators and manufacturers to test their system's environment for vulnerabilities, train their personnel, create knowledge exchanges for best practices, and define requirements for further improvement. A multi-sector testbed would primarily consist of private sector companies, and would cater to public sector goods and services such as the Water Management, Energy Sector, and Telecom Sector. Both the government and the private sector can learn from the use of such a testbed how to improve safety and security, also leading to improved policy making and regulation/legislation.

2 **Creating an appealing environment** that facilitates cooperation between the public and private sector and within the latter. Comprehensive legislation must be enacted, providing companies the conditions to work together and designate appropriate failsafe measures. At the moment, CI operators find it difficult to cooperate in knowledge sharing, procurement and tendering procedures due to restrictive legislation, myopic anti-trust laws, and unrevised policies. It is in the best interest of the public sector to create the right incentives to encourage the different CI companies to cooperate and nurture a more resilient CI environment. Although the national regulatory regime needs comprehensive changes, CI are not limited by national boundaries and are becoming a transnational issue.

3 **Fostering international cooperation** for CI protection. Addressing CI issues at the national level is only the first step towards tackling the risk of CI disruptions, cascading failures and common cause failures. CI operators that operate across borders demand the involved states to foster international cooperation and harmonization on CI protection. As states begin to rely on CI in neighboring states, it becomes more pressing to address CI standards, legislation, regulation and best practices at an international level. International cooperation should be fostered by CI operators and manufacturers and governments. This could be achieved through bilateral agreements between bordering and mutually-dependent states or through intergovernmental organization programs such as the European Commission's Critical Infrastructure Warning Information Network (CIWIN).

All three issues mentioned are necessary for a holistic approach to protecting CI from risk by making them more resilient. This list of recommendations should be taken as one element of a larger resolution, to be implemented concurrently. CI companies will only be able to cooperate further through comprehensive changes to regulation; the public sector will only foster resilient CI through cooperation of the private and public (critical) sector. The public and private sectors will only be protected from transnational threats by addressing this issue on the international level. For this report, we will delve into the current climate, the drawbacks, and the desired outcome of a multi-sector CI testbed in the Netherlands.

Knowledge exchange of the different known vulnerabilities will provide CI companies with patches and updates to the latest threats to their equipment, thus creating more resilient and safe CI.

6 – What is a Testbed?

A testbed is a platform where CI operators and manufacturers can test their hardware and software in a protected simulation environment. Also referred to as a *Sandbox*, a testbed is an isolated testing ground where IT and OT components can be tested for vulnerabilities.[12]

Demonstration SCADA hack bridge by Siemens during Cyber Security Weeks Innovation Room at HSD Campus

For CI, this means testing ICS components (i.e. SCADA, PLC, PCS, RTU) and the software that operates this equipment for bugs, exploits and possible cyber-attacks that can be carried out against them. These tests are carried out in protective environments that simulate the actual function of the CI component. Testing these components may cause them to malfunction or breakdown, meaning that they must be tested outside of their operational environment as to avoid economic loss or damages by disruption of services. For this reason, ICS components must be tested in environments where the systems are close to blueprint-like replicas of the original. Testbed platforms are also the space for certified specialists to carry out penetration testing and test the equipment against ISO levels and the ISA standard as to certify the equipment up to certain operational standards. Moreover, the resilience of alternate architectures can be assessed in practice with a testbed. Another function of the testbed is knowledge exchange. CI systems often use the same equipment components for different operations are applied in different sectors.

Knowledge exchange of the different known vulnerabilities will provide CI companies with patches and updates to the latest threats to their equipment, thus creating more resilient and safe CI.

'The goal of this CI testbed would be to share the burden across all industry sectors through a collective effort and break through silos of isolated investments in protection.'

7 – Current Climate for a National CI Testbed

The numbers of cyber attacks have soared over the last years, and the consequences of these attacks have become more expensive and harder to govern. At the international and national level, we can see how testbeds are emerging, what partnerships look like, and how they operate.

International Initiatives

There are currently few knowledge hubs for critical infrastructure testbeds around the world.

- In the United States, there are several testbeds at the state and national levels. At a smaller scale, there is the Idaho, Los Alamos, Sandia, Lawrence Berkley, and Argonne National Laboratories, which serve as testbeds and training facilities.[13] At the national level, the National Institute of Standards and Technology (NIST) declared it would create a testbed to examine ICS and SCADA systems to start in 2015. In addition to the NIST, the National SCADA Test Bed (NSTB) program was set up in 2003 for testing energy delivery systems.[14]
- Next to these, there is the USC-ISI DETER lab, funded by Department of Homeland Security (DHS), National Science Foundation and the Department of Defense. This lab facilitates cybersecurity experimentation and is primarily researcher oriented, in which available needed physical infrastructure and advanced tools are provided, incorporated, and shared.

DHS has recently extended an invitation to the Dutch research community to partake in the experimentation environment of Deter.

- Japan has created the Control System Security Center (CSSC), which is a company/association established in 2012 with the approval of the Japanese Ministry of Economics, Trade and Industry. Its mission is to strengthen technology and authentication security.[15] The CSSC is formed by 26 corporations with the likes of Mitsubishi, Toyota, Fuji Electric, McAfee, Hitachi, and Trend Micro. It is supported by eight member organizations in the fields of nuclear security, nuclear engineering, gas, tobacco, and industry.
- In the European landscape, there are currently several full-fledged SCADA testbeds for the Energy Sector. These include the Grenoble IOT-Lab (France), the CERN in Geneva (Switzerland), the European Joint Research Centre in Ispra (Italy), and the Italian National Agency for New Technologies, Energy and Sustainable Economic Development (ENEA) amongst others. In addition to the former testbeds, the European Commission has established an EU-Japan collaboration project known as FELIX (FEderated Testbeds for Large-scale Infrastructure eXperiments).[16] This program will define a common framework for federated Software Defined Networking (SDN) for the future of the internet across continents. The previous initiative is a testbed for Information Technology (the open internet); however it does not aim to resolve issues of Operational Technology.

Dutch Initiatives

The Netherlands had one of Europe's first testbeds, having constructed the High Flux Reactor (HFR) in 1955 as a testbed for the national nuclear power industry to gain further knowledge of nuclear technology through research.[17] Nowadays, the Netherlands is still pioneering in the area of testbeds. At the moment, it is common practice from CI companies to host their testbeds on their own premises. This form of testing leads to stove piped specialization of knowledge within a single company, within a single CI sector. This isolation prevents innovation in addressing vulnerabilities and risk. Through an open and collaborative effort, a multi-sector CI testbed can be set up in the Netherlands and hosted by The Hague Security Delta (HSD), the largest security cluster in Europe.

HSD has been created as a cluster to stimulate cooperation between businesses, governments and knowledge institutions in the Netherlands in order to improve security at the societal, organizational, and individual levels, and to stimulate economic growth in the form of jobs, qualified workforce, and revenues in the security sector. It focuses on the subjects of National Security, Cybersecurity, CI protection, Urban Security and Forensics. Over the year 2014 and 2015, the city of Hague has become a *Cybersecurity Gateway* in Europe, now hosting the NCIA, Eurojust, and the EC3. As such, The Hague is turning into the cybersecurity capital of Europe. Given the need to merge societal interests, economic performance and a drive for innovation, the HSD provides the perfect environment to host such efforts and incubate more resilient and cyber-secure CI. The development of a multi-sector testbed would provide the HSD's partners the opportunity to test their OT and IT against risk and vulnerabilities and would at the same time create a knowledge hub for best practices, serving the ambition of the HSD cluster. The goal of this CI testbed would be to share the burden across all industry sectors through a collective effort and break through silos of isolated investments in protection.

Currently, The European Network for Cybersecurity (ENCS) is one of HSD partners focusing on CI protection in the Energy Sector and is in the lead in terms of setting up a multi-sector testbed in the Netherlands. The ENCS was founded in 2013 as an answer to the absence of cybersecurity related training and testing facilities for CI and the lack of a knowledge-sharing network, specifically for ICS in the Netherlands. ENCS is an information sharing network for best practices, research and development, education and training, and has a testbed environment for PLC, RTU, and other CI equipment. ENCS's testbed operations consist of red team / blue team exercises, a test lab (i.e., testing of PLC in a simulated live environment), mitigation strategies, and recommendations on the latest vulnerabilities. ENCS's member list already consists of key players in CI sectors of the Netherlands, with companies in the Energy and Telecom Sectors such as Alliander, E.On, Enexis, and KPN. ENCS has also partnered up with consultancies, universities and research institutions such as TNO, Radboud University Nijmegen, Accenture, TU Delft, and Westland Infra.

Multi-Sector Involvement

CI testbeds generate information on vulnerabilities and best practices for CI sectors. Until now, CI testbeds only operate within one CI sector, meaning that the knowledge created becomes isolated within that specific sector. As the principles

of innovation indicate, cross-pollination of different inputs will always lead to new results. A CI testbed consisting of multiple CI Sectors would allow CI companies to share costs when testing equipment, would create cross-sector knowledge exchanges and would avoid duplications of efforts.

All sectors use and depend on ICS to some degree for their operations and delivery of goods and services. Although all sectors provide essential goods and services for society, within the Netherlands the three that emerge as the most critical are considered to be the Energy Sector, the Telecom Sector, and the Water Management Sector.[18] We narrow the scope down to these three CIs because the disruption of these CI sectors would trigger a cascading effect that would spill over to the remaining CI sectors. Failure of the Energy Sector would cause all services dependent on the energy grid to stop temporarily; the failure of the Telecom sector would halt all services that use GSM and CDMA communication including all communication traffic of the world wide web through the Netherlands; failure of the Surface Water Management could lead to the flooding of a substantial part of the country thus disrupting all CI Sectors within the affected zone. For this reason, we focus on the Energy, Telecom and the Water Management Sectors.

Presently, most research on CI testbeds concentrates on the Energy Sector. The Telecom and Water Management Sectors make use of similar ICS components and software and often may come to face the same vulnerabilities and types of threats. In addition to this, all three CI sectors have an interested in mitigating social and economic consequences, and investing in a testbed is a sustainable and synergetic choice. This cooperation can create a new mechanism to identify and establish industry standards for the CI equipment being used. This initiative will help both the manufacturers and end-users of these systems. In this scenario, manufacturers can produce more adequate technology using industry standards and operators of CIs and other infrastructures can make smarter cybersecurity demands regarding the technology needed. With this sort of initiative, regulation may be redundant.

Lessons Learned from CI Testbeds

Barely any research has been done on the effectiveness and lessons learned of CI testbeds.[19] As mentioned earlier, there are few international initiatives on creating testbeds for CI, meaning that lessons learned on this subject are still in their early stages and under development. Based on ENCS experiences, we have come to pick up on several issues that may hinder the development of a multi-sector testbed. The most pressing issues regard the mandate of the organization hosting the testbed and anti-trust laws that limit procurement opportunities.

The ENCS was originally founded as a platform for CI owners to become more cyber secure. After three years of operations, they are on their way to establishing themselves as a major player in testbed operations in the energy sector. The ENCS is legally a business with a non-profit status, owned by its members through shareholding. Due to this legal construction, the ENCS is limited in terms of what organizations it can interact with and vice versa. Given its status as a membership organization, some CI manufacturers have decided not become a member of the ENCS, as anti-trust laws prevented these companies from tendering for projects that would involve ENCS verification. There are also issues with the participation of the public sector, as government agencies may not become a member due to ENCS's legal status as a business. This limits the interaction between ENCS and the public sector to providing government staff with training and certifications against the latest cybersecurity threats.

In order to work around the anti-trust laws, ENCS has revised its membership model and will begin adopting the new category of Partners. In this model, business and organizations can interact with the ENCS on an equal standing, allowing CI manufacturers and CI integrators to participate in the ENCS testbed. For the ENCS to collaborate with public sector organizations, it would require a revision of its legal status as a non-profit business. This last point addresses a wider debate around the question of whether it is the private or public sector that should provide such cybersecurity to National CI. As the problem of CI vulnerability and risk affects everyone, it is important that both sectors share the responsibility equally through cross-sector collaboration, both across all CI sectors and across the public and private sectors.

A CI testbed should contain embedded monitoring functionalities to produce data records for ICS monitoring. This would provide CI companies with valuable information on how their systems function in the simulated environment and would help researchers in calibrating equipment.

8 – Requirements for Government and Companies

Given the absence of multi-sector CI testbeds worldwide, a list of clearly defined requirements for companies and governments does not exist yet. At the moment, we can only draw from examples from the Energy Sector and more specifically from the NIST report on *Performance Requirements and Specifications*.[20]

The report lays out US and international guidelines such as the IEC-62443 and NIST-800-82 guidelines.[21] The NIST sets out the following areas as attractive focus points for a testbed:

Security Approaches:
- Recommendations for perimeter network security
- Host-based security such as anti-virus
- User and device authentication
- In-line encryption
- Packet integrity and authentication
- Deep-packet inspection
- Zone-based security policies
- Cyber-physical redundancy
- Cyber-physical anomaly detection
- Robust/ fault tolerant control
- Automated fault recovery
- Distributed state estimation and validation

Networking Components and Protocols:
- IP-routable protocols
- Field bus (non-IP-routable) protocols
- Firewalls with deep packet inspection
- Managed industrial switches
- Network traffic monitoring

CI need optimization at three levels in order to improve the Operational Technology (OT) used in critical infrastructures and IT vulnerability:

1 Physical security, consisting of hardware security, the computer systems, routers, cables, and servers.
2 Network protection, protecting the communication between internal and external components be it corporate public/private corporate communication or controlling the ICS processes.
3 Software layer: comprising the operating system, BIOS, and programs that are being run for different purposes.

This optimization can be acquired through a combination of factors, such as upgrading legacy systems, implementing security standards for new equipment that gets integrated into existing systems, and creating solutions through product, process, or social innovation. Innovative multi-sector cooperation can help stimulate collaboration in this sector. It can encourage cross-sector cooperation, and it can carve the path for a knowledge network for the exchange of best practices and lessons learned.

A CI testbed should contain embedded monitoring functionalities to produce data records for ICS monitoring. This would provide CI companies with valuable information on how their systems function in the simulated environment and would help researchers in calibrating equipment. This collected information can also serve as a baseline to develop benchmarks to determine a company's standing compared to a standard.

Information sharing is a mindset that should be adopted by CI operators.

9 – The Envisioned Multi-Sector Testbed

A multi-sector CI testbed would need to provide CI companies a platform to test their software, their equipment, and train their professionals. The objectives of the testbed are an attempt at creating the adequate environment for CI companies to benefit from cross-sector cooperation. Information sharing practices must be carried out on different levels corresponding with the sensitivity of the information. The operational use of the testbed should lead to more CI company engagement and provide a network of highly qualified information security staff for CI protection.

Objectives

In this proposed testbed, CI companies from different sectors would host test labs in the same building. These test-labs would host the ICSs components and simulate their operational environment. For this aspect of the testbed, companies would need to invest in identifying the services they deem most important for testing, design a virtual duplication of the operational environment, and would then have to transmit the knowledge of how to run the proprietary software. Although the equipment being used will often be the same across the different CI sectors, the software and the operational environment will be different as it will most likely be custom tailored to specific operations center and the CI sector. At this level, knowledge exchange is highly limited between companies as the information on vulnerabilities and proprietary knowledge of the system's design is highly confidential.

Once the systems have been tested, and vulnerabilities have been found, researchers can then test for the same conditions in other environments as to find if the same vulnerabilities are present. Vulnerabilities and exploits found from CI equipment can reveal the levels of security that the CI manufacturers or CI software producers are implementing into the products. This would help strengthen databases of vulnerabilities and assist in the creation of benchmarking tools to assess a products quality. In the longer term, it may be envisioned that this testbed would provide CI equipment certifications indicating top-quality security compliance.[22]

The testbed should comply with these minimum expectations:

- Create a platform that has hosts test labs for different CI sectors.
- Should generate knowledge that can be used towards creating solutions for CI equipment.
- Should train information security staff on the latest threats and exploits in CI components.
- Should establish a network of highly qualified information security staff.
- Should provide periodical reports to CIOs and information security personnel at confidential levels when security solutions are not found yet.
- Should provide open and freely available security reports along with the security solution to third party CI companies Should turn security requirements into new industry standards.
- Should educate CI companies in best practices and lessons learned drawn from across all sectors.
- Should establish cooperation and information sharing among participating partners.

Information Sharing

Information sharing is a mindset that should be adopted by CI operators. In the envisioned testbed, information can be shared on different levels depending on the participation of the partner. At the most operational level, in the test-lab, information should remain highly confidential between the CI operator and the researchers. At this level, the information revealed by the testing will be of high-detail and may reveal exploits that may compromise the CI operator's services or production of goods. This information would then be vital for the patching of the CI components at risk, and for inspecting if other CI operators have equipment that suffer from the same vulnerabilities.

The sensitive information on the proprietary systems may be left out, and the core exploits and lessons learned from the testing may be shared with other partners of the CI testbed. It would be envisioned that the research generated would produce periodical reports for CIOs, CERTS and other information security staff of the CI companies. These reports would highlight the latest threats and vulnerabilities, meaning their circulation would be held confidential and under the discretion of the partners.

Upon patching the IT and OT components, the exploits and vulnerabilities discovered should be published in the form of white papers in order to stimulate open research of the affected components. This should also encourage other CI companies with the same vulnerabilities to update their own CI components. Providing open information to other CI companies on exploits along with the security solutions would help these companies assess the security standards of their own CI components and may provide incentives for these CI companies to collaborate in a multi-sector testbed.

Operating the Testbed

The envisioned testbed should function as a network hub. Members of the testbed would contribute annual or monthly fees for the daily operations of the testbed. Fees should be tailored to the demands of the CI companies, the size of the industry, and should be proportional to the use made of the testbed. In regards to staff of the multi-sector testbed, CI companies would have the choice of seconding their information security staff to the testbed or would need to make use of the testbed researchers available. Members CI companies would then be eligible to participate in seminars and would be eligible to send their staff to training seminars. These seminars would be beneficial for information security staff, not only in terms of vulnerability and threat awareness, but also as a valuable networking opportunity with other information security staff from other CI companies and thus create and informal network of highly qualified cybersecurity professionals.

Deloitte demonstrates Industrial Controle Systems vulnerability of critical infrastructures during Cyber Security Weeks Innovation Room at HSD Campus

The creation of this testbed would promote innovation in the CI environment and would enable cross-sectoral collaboration between the different CI sectors, and across government, private companies, and research institutions.

10 – The Next Steps

Creating a multi-sector testbed in The Hague will enable CI companies in the Netherlands and the different Dutch Government agencies to improve their security awareness, their knowledge of cybersecurity risks, and improve daily operations of the CI sectors that are essential for the functioning of modern society.

The creation of this testbed would promote innovation in the CI environment and would enable cross-sectoral collaboration between the different CI sectors, and across government, private companies, and research institutions. This initiative will have the potential to enable international cooperation in this field and thus foster safer and more secure CI for all Europeans.

Endnotes

1 European Commission, COM(2004) 702 final, on Critical Infrastructure Protection in the fight against terrorism.
2 Voortgangsbrief Nationale Veiligheid, Minister van Veiligheid en Justitie, 13 mei 2015, Kamerstukken II, 2014-2015, 29517-96.
3 The criticality status of telecommunications and ICT sectors are still being reevaluated and are part of an ongoing debate.
4 A *patch* refers to software intended to update a computer program or it's supporting data in order to fix it or improve it. Patches are a common form of updating systems to prevent the latest vulnerabilities.
5 There is an extensive market for services and for vulnerabilities. Zero-day exploits for example, can sell for millions of dollars in the black market, and have been used for sophisticated attacks such as the Stuxnet attack.
6 A *Script Kiddy tools* is a derogatory term originated by expert programmers and hackers to denote scripts that can be executed by amateurs with *1-click* interfaces.
7 There are more acts of sabotage such as physically cutting cables and the insider threat; however they are not included in this report.
8 For more details about the Stuxnet case study, see Symantec's 2011 analysis of the computer code *W32.Stuxent Dossier*.
9 The German Steel mill attack is currently the second occurrence of a cyber attack causing physical damage. For the full article, see *A cyberattack has caused confirmed physical damage for the second time ever* in wired.com. http://www.wired.com/2015/01/german-steel-mill-hack-destruction/
10 According to the Dutch Bank Association (Nederlandse Vereniging van Banken – NVB) cyber attacks on the Banking Sector amounted to nearly 35 million euros. See NVB's position paper *rondetafelgesprek Online Betalingsverkeer* of 30 may 2013.
11 For more details on this incident, see The Union for the Co-coordination of Transmission of Electricity's (UCTE) reporton *System disturbance on 4 November 2006*.
12 It is important to highlight the distinction between Operational Technology (OT) and Information Technology (IT) in the Critical Infrastructure domain. IT pertains to the information being dealt with in the CI. This will translate to the communication running through the fiber optic cables, the instructions being delivered to the ICS systems, the data being sent over satellites, and the messages being sent over phone towers. OT on the other hand is vehicle for IT, in the sense that OT is the technology that enables the IT. OT would therefore be the means in which the data/information/communication is delivered
13 More information on the US testbeds can be found on the website of the Office of Electricity Delivery and Energy Reliability under *National SCADA Test Bed*.
14 For additional details of the NIST Testbed: http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed
15 The CSSC website provides extensive information on their research and development models, for more information see www.css-center.or.jp/.
16 The FELIX project holds partners from EU Member States such as Poland, Italy, Spain, the Netherlands, Germany, and Belgium, and two partners in Japan.
17 For more information on the High Flux Reactor at Petten please see www.world-nuclear.org/info/Country-Profiles/Countries-G-N/Netherlands/.
18 By identifying these three sectors, we are in no way ranking the importance of the CI sectors, but are highlighting a relevance hierarchy in the sense that one sector may be more dependent on the other. All CI Sectors are equally of vital importance.
19 It is important to note that though there is very little research done on CI testbeds, there is considerable amount of research done on IT testbeds. These sorts of testbeds run penetration testing to uncover exploitable computer systems.
20 For the complete list of recommendations, see NISTS's Guide to Industrial Control Systems (ICS) Security, special publication 800-82 of June 2011.
21 See http://http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
22 These efforts would have to complement ongoing initiatives in various other platforms such as the Working party for Instrument behavior (WIB), focused on the process industry, and other international standardization bodies.

Notes

Publication information
Securing Critical Infrastructures in the Netherlands: Towards a National Testbed

ISBN/EAN: 978-94-92102-30-0

A publication of
The Hague Security Delta
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
T +31(0)70 2045180
info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL

Authors
Nicolas Castellon and Erik Frinking

Design
Studio Koelewijn Brüggenwirth

Drukker
ANDO Graphics

Photography
Hilbert Krane
Dataplace Alblasserdam
Frank de Roo
Aerialtronics
Third

The authors would like to thank the following people and organizations for their valuable contributions: Gerben Klein Baltink (MKB Cyber Advies), Benessa Defend (ENCS), Maarten Hoeve (ENCS), Robert Liesveld (KPN), Eric Luiijf (TNO), Kees Mouwen (KPN), Bram Reinders (Alliander).