Understanding the Strategic and Technical Significance of Technology for Security

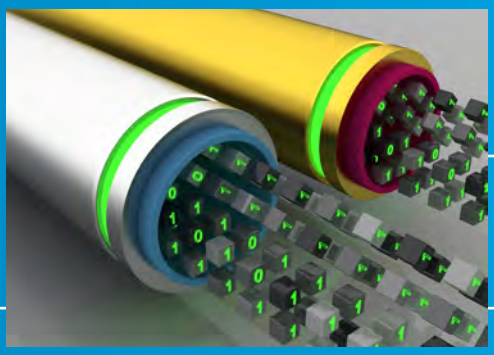
The Case of Data Diodes for Cybersecurity

The Hague Security Delta

Understanding the Strategic and Technical Significance of Technology for Security

The Case of Data Diodes for Cybersecurity

The Hague **Security Delta**




BAD
GOOD

Table of Contents

1 – Introduction: Technology and Cybersecurity

Our society is undergoing a digital transformation. The characteristics of this transformation are determined by the convergence of technologies and social activities that blur the boundaries between physical, digital, and biological systems. Moreover, the speed of this transformation is dizzying. Developments such as 'big data', 'cyber crime', 'blockchain', 'autonomous systems', artificial intelligence (AI), and 'smart cities and societies' will soon be replaced by another pantheon of terms and themes.

These technological breakthroughs result in major societal, social and economic changes, leading to considerable challenges, not least in relation to security, such as:

- How do we establish safe and secure access to, and use of, the Internet?
- How do we prevent the loss of legitimacy and integrity of digital activities?
- How do we stimulate the use of accountable and explainable algorithms?
- How do we define and protect privacy of citizens?
- How do we balance individual, societal, economic, and ethical interests?

In 2018, the Dutch government presented a new innovation policy framework, which focuses on achieving mission-oriented innovation to provide answers to these challenges and make use of the opportunities.[1]

The policy is based on setting up collaboration, already initiated within the Top Sectors[2], in four central themes:

- energy transition and sustainability;
- health care;
- agriculture, food, and climate; and
- security.

Innovations in these fields require dedicated investments that need to translate into applicable technological breakthroughs. Thus, the Dutch Cabinet intends to heavily invest in development of key technologies such as photonics, artificial intelligence, and nano-, quantum and biotechnology. All in all, societal and economic possibilities for the security domain seem ample.

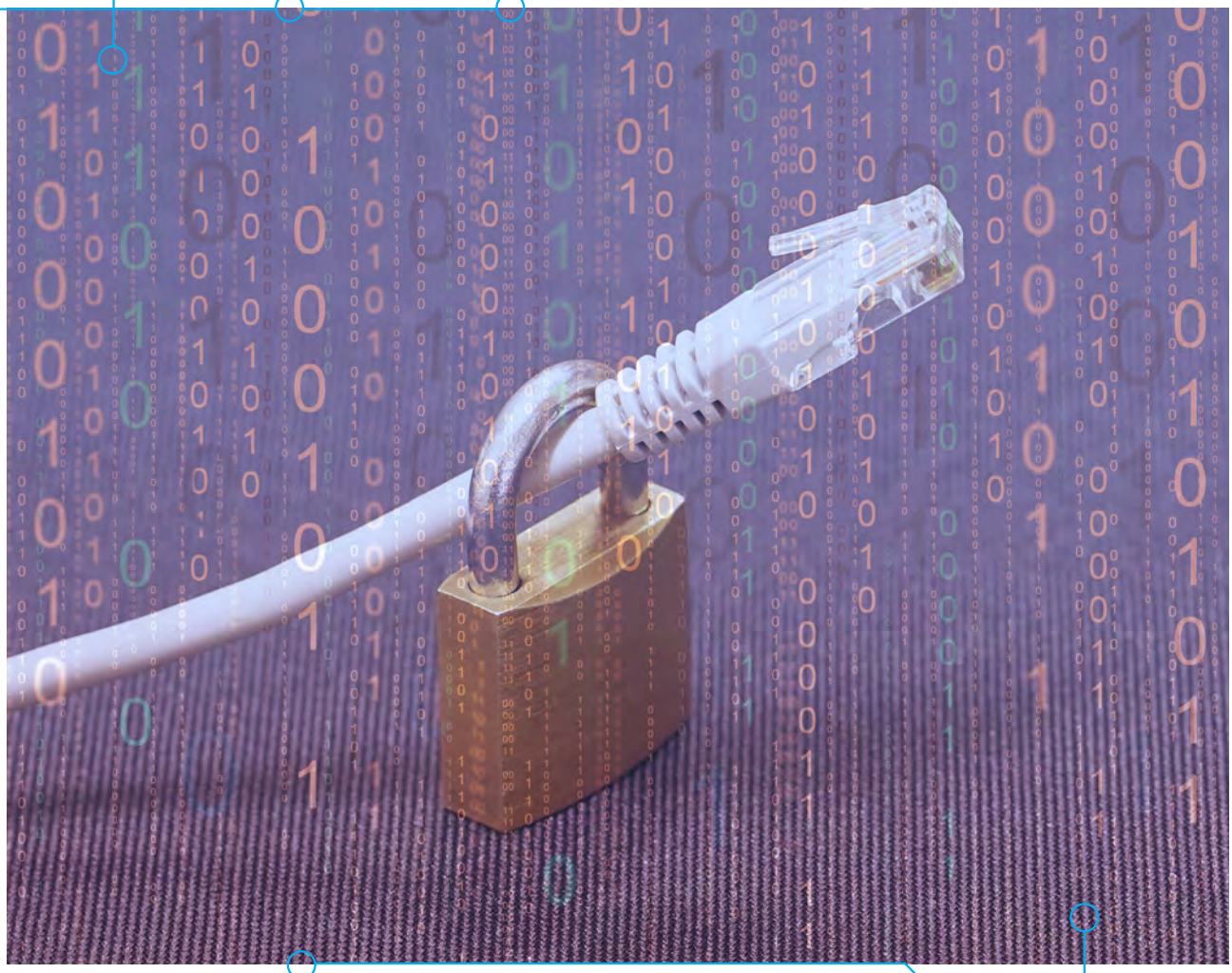
Still, recent publications (Cybersecurity Assessment Netherlands 2018 [CSAN2018],[3] the third National Cybersecurity Research Agenda [NCSRA III])[4] and discussions in existing environments (e.g., HSD) show that insufficient use is made of these opportunities, often as a result of a lack of awareness, and that security concerns – one of the main themes of the Dutch Cabinet – are not a top priority.

1 "Kamerbrief over Innovatiebeleid en de Bevordering van Innovatie: Naar Missiegedreven Innovatiebeleid met Impact." Ministerie van Economische Zaken en Klimaat, July 13, 2018. https://www.rijksoverheid.nl/documenten/kamerstukken/2018/07/13/kamerbrief-naar-missiegedreven-innovatiebeleid-met-impact.

2 In February 2011, the Dutch government announced the Top Sectors approach, a form of industrial policy which focuses public resources on specific sectors and promotes coordination of activities in these areas by businesses, government and knowledge institutes. The nine sectors chosen are: horticulture and propagation materials, agri-food, water, life sciences and health, chemicals, high tech, energy, logistics, creative industries. See: "OECD Reviews of Innovation Policy: NETHERLANDS." Organisation for Economic Co-operation and Development (OECD), 2014. http://www.oecd.org/sti/inno/netherlands-innovation-review-recommendations.pdf.

3 "Cyber Security Assessment Netherlands 2018." Ministry of Justice and Security, August 7, 2018. https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html.

4 "The National Cyber Security Research Agenda (NCSRA-III)." dcypher, June 5, 2018. https://www.dcypher.nl/sites/default/files/uploads/documents/NCSRA-III_0.pdf.



Members within the HSD community have requested to raise attention to a number of these developments that could intrinsically improve the cybersecurity landscape, in the short or longer term:

1 The short-term potential of specific data diode technology;
2 Unsupervised learning within the domain of artificial intelligence on the mid- to long-term;
3 The longer-term potential of quantum technology.

This paper addresses the first topic.

The ultimate objective of this study is to investigate whether, and how, data diodes can contribute to a safer cybersecurity landscape. To do so, we will try to answer the following questions:

- What are current developments in the supply of data diodes, including within the open source domain?
- What business process components can be made significantly more secure by using data diodes?
- How are organizations experiencing the use of data diodes and what bottlenecks do they encounter?

The paper first provides an understanding of data diode technology and its playing field. Subsequently, it shows an overview of advantages and disadvantages in the use of data diodes. Finally, new developments in this domain are presented.

We conducted our analysis primarily on the basis of existing literature (official documents and secondary sources) and available data. Having identified our knowledge gaps, desk research was supplemented by a limited number of interviews with relevant stakeholders to help us get a better understanding of strengths and weaknesses of the data diode technology, the size of the market and of the customer base, as well as of the existing partnerships and collaborative initiatives (see Annex 1 for the interview protocol).

To assess the potential of data diode technology, we looked at it from two dimensions;

- SWOT: This analytical framework was used to evaluate the problems which data technology addresses, as well as solutions it provides. SWOT stands for strengths, weaknesses, opportunities, and threats.
- PESTEL: This analytical framework was used to identify external factors that affect and exacerbate the development of data diode technology. PESTEL stands for political, economic, social, technological, environmental, and legal factors.

2 – Context

In the realm of cybersecurity, there is a considerable number of attack vectors and means (such as email attachments, pop-up windows, deception, chat rooms, viruses, USB sticks, remote access, etc.) for adversaries to breach the confidentiality, integrity, and availability of a network and the data that resides on it. Entry to a network can be forced to alter or disrupt its operations, to wipe data, or to use it for illegal purposes. All of these attacks can lead to significant damages for the victim.

In the Industrial Internet of Things (IIoT), these cybersecurity attack vectors present a challenge to sensitive, high-value networks that must remain protected and at the same time open up to provide and incorporate data flows to authorized users on demand.

> *In June 2017, NotPetya malware was used to infiltrate Ukrainian power plants and other critical infrastructure organizations, causing them to shut down. The ransomware was downloaded onto computers using updates for the widely used Ukrainian accounting software, MeDoc, which had previously been hacked. Once attackers were able to access information systems at computers within the general environment, they were able to affect the connected operating technology (OT) and shut down factories at will.*[5]

It is a generally accepted cybersecurity strategy to implement a layered security approach by compartmentalizing or segmenting areas that have different trust levels. There is a variety of means to defend networks against external threats, such as firewalls (software-based), stand-alone networks (physical), or data diodes (hardware). As we will highlight below, they each have their own strengths and weaknesses, and are more or less suitable in different settings and circumstances.

In effect since 9 November 2018, the Network and Information Systems Security Act's (Wbni)[6] mandate is to increase the digital resilience of the Netherlands in general, and in particular, its critical sectors. This law, which constitutes the Dutch implementation of the EU NIS directive,[7] is focused on mitigating the consequences of cyber incidents in these sectors and subsequent disruptive effects in society. It requires providers of critical services or digital services to use appropriate and proportional means to protect their ICT against incidents. In the case of serious incidents, they are required to report these to their national authorities. Especially in these sectors, data diodes provide a level of security that could meet the identified risks. However, experience with, and implementation of, these techniques in other sectors is still very limited.

5 Brewster, Th.. "NotPetya Ransomware Hackers Took Down Ukraine Power Grid." Forbes, July 3, 2017.

6 "Wet van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen)." Overheid.nl, October 17, 2018.

7 "Wet van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen)." Overheid.nl, October 17, 2018.

3 – What is Data Diode Technology and How Does it Work?

As stated in section 1, there are three fundamental objectives that guide policies for cybersecurity within an organization;

- confidentiality: ensuring that sensitive information is not shared with those who do not have access to it;
- integrity: maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle; and
- availability: making sure that data is available without any glitches, such as maintaining a backup copy of files and providing adequate bandwidth for communication.[8]

There are numerous real-world examples of how these fundamental objectives have been breached.

Break of confidentiality classified government information
A cyberattack on the United States Office of Personnel Management in 2015 provides another interesting example. Attackers posed as employees of a subcontractor – KeyPoint Government Solutions – to gain access to personal information, such as Social Security Numbers, past addresses, and security clearance files from government employees.[9]

Break of confidentiality of business proprietary information
Also, more ordinary business monitoring processes might be tied to organization's more confidential systems. For example, a North American casino was hacked via an internet-connected fish tank in 2017, resulting in the theft of 10GB of data.[10]

Break of integrity in critical infrastructure
During the cyberattack on Ukraine's power grid in 2015, workers in power generation centers could remotely log into the SCADA systems without two-factor authentication. Once hackers stole workers' credentials, they were able to set up a command and control unit within the operations unit of the system.[11]

Disruption of network availability
In 2016, a Mirai botnet – comprised of 45,000 IoT bots – executed a massive DDoS attack in the United States, leaving much of the internet inaccessible on the East Coast of the United States. Besides the websites (e.g. Twitter) and web services (e.g. PayPal), Verizon Communications services from broadband to cell phone were also disabled, limiting the means of communication for the area concerned.[12]

Data diode technology can provide cybersecurity while at the same time providing network connectivity. Data diodes traditionally serve to protect secrets and to protect assets. When a data diode is deployed to protect secrets, confidentiality takes priority over integrity. When protection of assets (typically industrial systems) is the primary goal, integrity and availability are essential.[13]

The major benefit of data diodes is the possibility of linking an insecure (part of the) network to a secure (part of the) network while maintaining the confidentiality or integrity of the most secure network. These networks

8 Also referred to as the C.I.A. triad

9 Koerner, Brendan. "Inside the Cyberattack That Shocked the US Government." *Wired*, October 23, 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

10 Schiffer, Alex. "How a Fish Tank Helped Hack a Casino." *The Washington Post*, July 21, 2017. https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?noredirect=on&utm_term=.303ae5e989ad.

11 Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired, March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

12 Carter, Candice. "Critical Infrastructure and Cyber Security." Incapsula Blog, October 30, 2017. https://www.incapsula.com/blog/critical-infrastructure-cyber-security.html.

13 Teepe, Wouter, and Colin Robbins. "Protecting Confidential Information Using Data Diodes." White Paper. Fox-IT, July 2014. https://www.fox-it.com/datadiode/wp-content/uploads/sites/9/2015/02/Fox-DataDiode-Protecting-confidential-information-using-data-diodes-EN1.pdf.

can contain operational systems (e.g., making factories perform), classified information (e.g., storing intellectual property or state secrets), monitoring systems (e.g., interpreting the meaning of sensor data), accounting obligations (e.g., collecting personal and financial data), and many more. The less secure networks can assemble or interpret the information provided by more secure networks. They may also be simply connected to each other for efficiency or legacy reasons.

3.1 What does a data diode look like?

Three properties describe a data diode:

- Its mode of configuration;
- Its level of integration of hardware and software;
- Its use of communication protocol.

3.1.1 Configuration

A data diode is a hardware-based electronic device designed with two separate circuits – one transmit-only, and one receive-only – which physically constrain the transfer of data to one direction only. Data is transferred by using proxy servers, which are attached to the data diodes and use protocols so that the information can be sent through. As such, data diode products (or: unidirectional network gateways) offer one-way only communications.

The figure below provides a simplified overview of how the two basic modes of configuration work.

This allows for data to travel from low to high security networks or vice versa without being able to travel back. A data diode configured as receive-only is believed to constitute the best possible technology to protect the *confidentiality* of data (i.e., to prevent leakage or exfiltration of sensitive data).[15] Data diodes configured as transmit-only ensure the *integrity* and *availability* of the data (i.e., protect the high security network from external attacks). However, a unidirectional network connection in and of itself does not prevent attacks that may impact the availability and integrity of the *downstream network* in both configurations. It does, however, prevent denial of service attacks (DDoS) at the high-secure environment in the transmit-only configuration.[16]

Imagine a nuclear power plant's operational network that needs to communicate data to a less secure network, such as its corporate control and communications network or an external network of a maintenance firm. This could be information from a sensor that measures the temperature of a material, which helps the controller to decide whether adjustments to the operations need to be made.

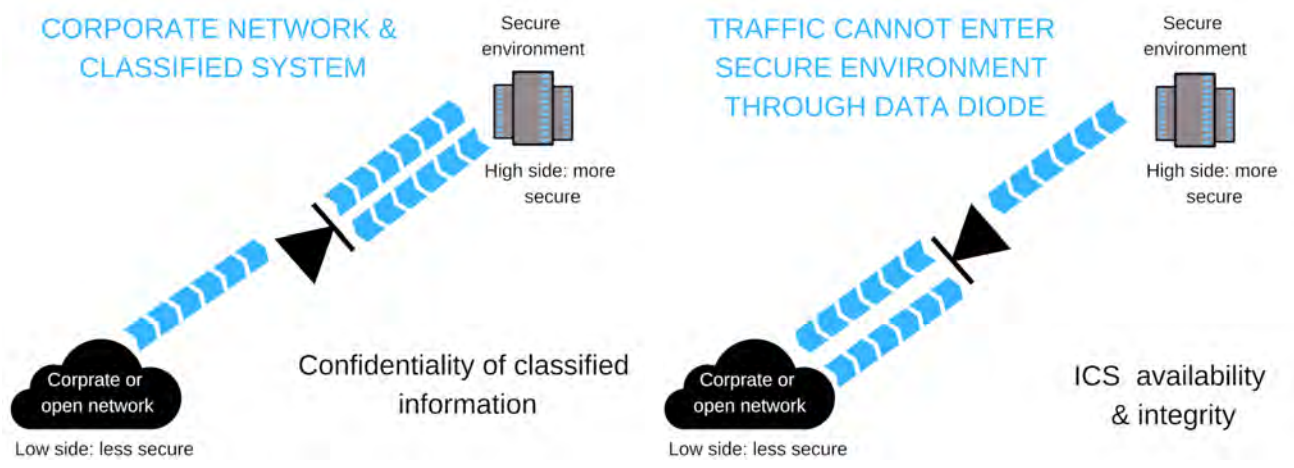
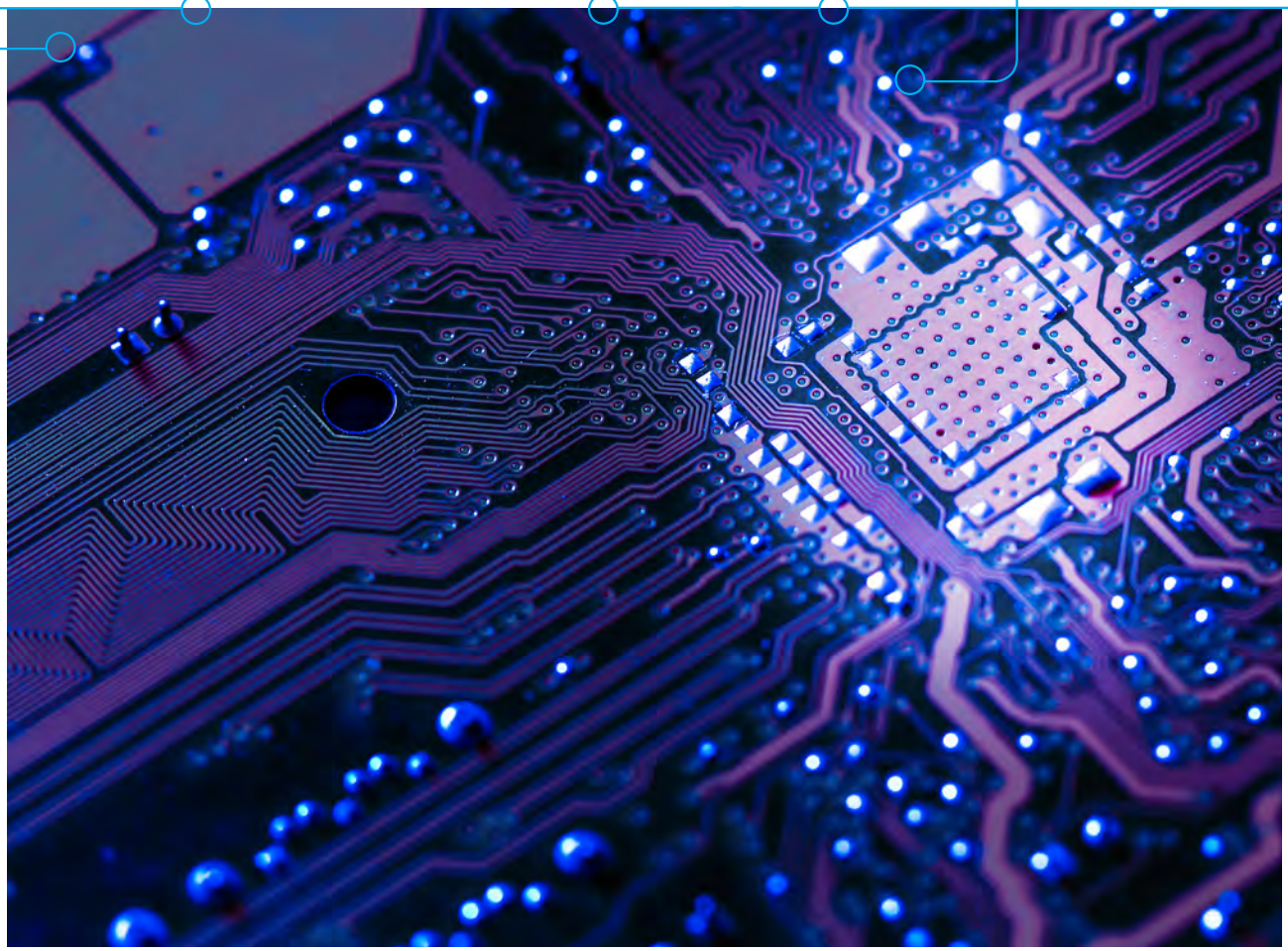


Figure 1 **Two basic modes of configuration of data diodes: receive-only and transmit-only.[14]**

14 Scott, Austin. "Tactical Data Diodes in Industrial Automation and Control Systems." SANS Institute InfoSec Reading Room, May 18, 2015. https://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automation-control-systems-36057.

15 Teepe and Robbins, "Protecting Confidential Information Using Data Diodes."

16 Ibid.



Thus, transmitting the data is pertinent as it helps the control center to assess the operations in real-time. However, sending back data across the same path, which might affect the operations, intentionally or unintentionally, is not desired.

This is a clear-cut example of a transmit-only data diode in which data flows from a more secure portion of the network to a less secure portion and no other traffic can enter the more secure side of the network.[17]

In contrast, an example of a receive-only data diode would involve a defense or intelligence system that needs to have a network connection to receive data from the less secure network. In this example, the receive-only diode would restrict the flow of information to only receive data from this less secure side of the network and not the authorized or unauthorized transfer of highly classified information from the highly secured side.

3.1.2 Integration of hardware and software

For the full functionality of data diode technology, the hardware component needs to be supported by a software environment. While a data diode allows for a unidirectional connection, many communications require more than simply a pathway: they require acknowledgement or other specificities of some sort to send through their data.

Thus, in addition to the transmit-only or receive-only configurations, data diodes might also be designed differently: some integrate software to manage communication into the hardware (comparable to software or system on a chip), others explicitly separate the software component from the hardware. In most cases, servers need to be installed on both networks to provide the ability to communicate with their immediate environments.

17 A commonly made distinction is that between information technology (IT) systems and operational technology (OT) systems. The former technology is used for processing information, the latter for monitoring or altering the performance of a physical system, such as (parts of a) power plant, by controlling valves or engines.

3.1.3 Use of protocols

Protocols, operating as sets of rules, allow computers to communicate and to transmit information between them. The software environment is needed to convert bidirectional protocols to a unidirectional protocol to allow data to be sent over a diode, and to ensure the security of any information that *is* allowed to flow through a data diode.[18]

Within computers, TCP/IP is perhaps the most commonly used set of protocols. There are two essential parts to TCP/IP communication between computers: the payload and the protocol. Hackers aim to take control of these protocols by sending bad traffic control data (protocol metadata), which gives them control of the system.

As Table 1 shows, protocol breaks and proxies are integral to the use of data diodes. This is because they can allow a data diode to have more communicative functionalities than it would otherwise have. It allows for certain types of computer communication that normally require acknowledgements that a data diode cannot give without a separate proxy. Another reason why a protocol break is essential for a data diode lies in its ability to segment the high security system from the low one, not only allowing for communication, but doing so in a way that protects the integrity of the high security system.

Because many protocols such as SMTP and HTTP require the receiving system to acknowledge the movement of data, a data diode alone would not be able to work with such protocols unless it had an additional proxy server, which may or may not be integrated with the diode itself. As such, both configurations of data diodes also often include protocol breaks or proxies, which separate the traffic control data from the payload. As data diode technology is an IT product, it falls under the purview of the Evaluation Assurance Levels (EAL). The EAL certification system measures the extent to which an IT product follows the completion of a Common Criteria for Information Technology Security Evaluation (CC). Different EAL levels refer to different levels of testing that a system has undergone, such as penetration or functional testing, or whether it has design documentation and design analysis.[19]

EAL certification can be quite expensive as formal verification can be both a lengthy and high-cost process. The different configurations as described above will affect the level of certification. For example, data diodes with the highest possible certification level have strictly separated the hardware component from the software aspects. Also, changes in technology or materials used might upgrade or downgrade the level.

Proxy Servers	Protocol Breaks
A proxy server is a general term for a system that acts as an intermediary between two other systems. Data diodes may have the option to include proxy servers, which can send acknowledgement receipts for protocols that require them, such as TCP/IP communications. If proxy servers are used, they are generally installed at both ends of the network.	Protocol breaks contain two components. The first component strips the traffic control data from the actual data and the second sends that data to the receiving system. Even if a system stripping traffic control data is compromised, the data diode protocol would simply ignore it and remain secure. Data diodes can include protocol breaks as an add-on in a piece of software. This ensures that if data is sent through the diode appropriately, it does not contain malware.

Table 1 **Add-ons for data diode technology.**

18 "Data Diode vs Firewall: How Do They Compare?" Fox-IT, July 6, 2018. https://www.fox-it.com/datadiode/2018/06/07/data-diode-vs-firewall-compare/.

19 "The Common Criteria." Common Criteria Portal. Accessed January 21, 2019. https://www.commoncriteriaportal.org.


GOOD
BAD

4 – Strengths and Weaknesses of Data Diode Technology

Having described the functionalities and configurations of data diode technology, this chapter will focus on its specific strengths and weaknesses, including in comparison to its alternatives.

To date, there have been no reported cases of data diodes being bypassed or exploited, which in itself would indicate a certain intrinsic hardiness.[20] At the same time, the proliferation of the technology is still limited.

4.1 Strengths

The strongest feature of data diode technology appears to be **its hardware aspect.** With this technology, there is no memory, settings or parameters that can be changed or hacked, which give software solutions inherent weaknesses.[21] As was presented in the previous chapter, there are versions of data diodes available with integrated software components, which are vulnerable to attack. In that sense, not all data diodes are equal.[22] According to the interview results, software-based data diodes are very hard to protect and thus cannot be acknowledged as being a true data diode.[23]

By using a hardware system, **both configurations of data diodes remove, to a large extent, the possibility of user error.** For example, while a firewall might protect the data itself from harm, it does not protect against a user clicking on malware that would expose information on a high security network. Data diodes simply prevent that possibility from occurring.

Another strength resulting from their hardware composition is the **ability of transmit-only data diodes to protect and preserve legacy systems**. Many systems that drive critical infrastructure operate on older hardware and/or software systems, even going back as far as Windows 3.1. By using data diodes, legacy systems can be protected without overhauling the entire operational system. This is a considerable benefit as these systems tend to be incrementally built over the period of many years (i.e., the logical design of the big picture is often unavailable) and cannot afford to have their operations interrupted.

Applicability of data diode technology goes beyond the realm of critical national infrastructure. Many election systems run on old software and machinery, which make them vulnerable to cyberattacks. By adopting data diodes into this kind of legacy system, it is possible to gain more security for the system without having to take them offline or similarly update them and possibly expose them to more vulnerabilities.

No less important, a third strength of transmit-only as well as receive-only data diodes lies in **their ability to ensure security in insecure systems.** Cyber attackers choose to assault network systems depending on what kind of weakness they present. Two of the most prevalent types of cyberattacks are DDoS attacks and buffer overloading. DDoS attacks rely on two-way traffic and therefore are unavailable to hackers wishing to infiltrate a transmit-only data diode system. On a receive-only configuration, data diodes would need to rely on the installed software, which would mark such an attack as irregular or be constrained by the data flow limitations that some data diodes possess.

20 Scott, Austin. “Tactical Data Diodes in Industrial Automation and Control Systems.” SANS Institute InfoSec Reading Room, May 18, 2015. https://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automation-control-systems-36057.

21 These include software complexity, the current average rate of errors per Line of Code, etc.

22 Menoher, Jeffrey. “Not All Data Diodes Are Equal.” White Paper. Owl Computing Technologies, September 6, 2013. http://www.scadahackr.com/library/Documents/White_Papers/Owl%20-%20All%20Data%20Diodes%20Are%20Not%20Equal.pdf.

23 “Fox-IT Data Diodes One-Way Traffic Keeps Secrets Safe.” Fox-IT, 2016. https://www.fox-it.com/datadiode/wp-content/uploads/sites/9/2016/07/Fox-DataDiode-One-Way-Traffic-keeps-Secrets-Secret-023-101-EN.pdf.

Furthermore, long-term operating costs are low. After initial investment of purchase and system integration, the savings in maintenance and administration costs make the data diode an efficient network security solution in the long run.

Another strength of data diodes is the manner in which they compartmentalize cybersecurity risk. When using a receive-only data diode with a protocol break, for example, there will be no data leakage despite the downstream network being exposed to potential integrity problems.

4.2 Weaknesses

The high cost constitutes one of the biggest challenges to implementing data diode technologies. Depending on the specificity of the request, Owl Cyber Defense estimates that a data diode can cost anywhere from 30,000 EUR to 150,000 EUR.[24] Fox-IT estimates that the lowest certified configuration of a data diode would still cost 15,000 EUR.[25] Although diodes and solutions are available at a lower cost, they often lack government approval or certification. Some cyber professionals consider cheap versions of data diodes currently as vulnerable and untrustworthy.[26]

Furthermore, many companies do not see the implementation of these technologies as worth the investment versus the assets they are protecting or against the level of security that firewalls provide. The Netherlands' Digital Trust Center, which is supporting small and medium-sized enterprises to secure digital operations, does not (yet) consider data diodes as part o f the basic cybersecurity toolbox, likely because of their cost and (in)accessibility for many companies.[27]

In addition, data diodes require specialized knowledge and skills to install, which clients do not always possess (data diodes can take up to two days to install). Configuration and monitoring may also add to the expense and user complexity of the device, potentially discouraging organizations with fewer in-house ICT skills. Installation costs, however, vary depending on the vendor.[28]

Up until now, data diodes have been relevant primarily for critical national infrastructure or industrial control networks (ICS/SCADA) due to compliance requirements in countries such as the United States. **In Europe, compliance is neither prescribed nor required, which constitutes one of the reasons why data diodes are not commonly known**, used, or well understood outside of national critical infrastructure organizations.

Another challenge associated with the use of data diode technology is that the vast majority of modern communication protocols require two-way communications in order to function. **Data diodes do not work with standard TCP/IP protocols**, only with protocols that are unidirectional by design, and that do not require confirmation or acknowledgment of receipt as explained in Chapter 3.[29] Because of protocol implementation, some **data transfers may be slow and lack reliability**. These slower data diodes can have bad quality of service and reliability, although not all data diodes operate in this fashion.[30] Data sent over a data diode must be carefully filtered because the amount of data that can be sent is limited. Furthermore, transmit-only data diodes cannot read whether or not data has been successfully received, which may lead to obstructed information flows and data loss.

24 "Data Diodes for CBarry, Courtney. "Data Diodes for Cyber Security." TechSurveillance Magazine, March 2012. http://courtneybarry.com/Images/TS_Data_Diodes.pdf.

25 Based on interview results

26 Robbins, Colin. "Can You Trust a $1612 Data Diode?" CyberMatters (blog), March 12, 2013. https://cybermatters.info/2013/03/12/can-you-trust-your-1612-diode/.

27 "Digital Trust Center," n.d. https://www.digitaltrustcenter.nl/.

28 Scott, Austin. "Tactical Data Diodes in Industrial Automation and Control Systems." SANS Institute InfoSec Reading Room, May 18, 2015. https://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automation-control-systems-36057.

29 Menoher, "Not All Data Diodes Are Equal."

30 Menoher, "Not All Data Diodes Are Equal." 3

Albeit secure by design, and stored within a physically secure environment, data diodes are prone to human error as well as to physical tampering. The human factor is always the weakest link in any security program. A user on the high security level network can accidentally or deliberately breach the confidentiality of classified information by stealing data through a USB stick, for example.[31]

Diodes do not prevent people from printing documents, or from sharing the information in a different manner. If the high security network has a portal for a USB stick or another portable media device, misconfiguration can occur if, for example, an employee inserts a USB drive that has not undergone rigorous anti-malware scrutiny.

31 Gedrojc, Bartek. "Fort Fox Hardware Data Diode: Security Target: Common Criteria FFHDD – EAL7+." White Paper. Fox-IT, June 3, 2010.

4.3 Data Diode, Firewall and Air Gap: How Do They Compare?[32]

To ensure their security, networks (be it IT, OT or any combination, see also footnote 17) can be fully separated via an air-gap, joined by well-configured firewall(s), or connected by various configurations of data diodes. There is an ongoing debate about the appropriate balance of the three solutions that protect highly sensitive data and networks best. The most comprehensive solution is likely one that utilizes one or more of these strategies to control for multiple attack vectors.

An **air gap** is a physical disconnect between a high-security system and a low-security system. Because a truly air-gapped network is completely isolated from the outside world,[33] data leakage or malware entry is unlikely.

Risks involved with air gaps revolve primarily around bad user behavior, or when malware enters the system by means of removable drives, such as USB flash drives, plugged in by insiders.[34]

However, the biggest drawback is that air gaps deny the possibility for systems to exchange information in real time or to provide services remotely as modern internet communications can provide. Air gap models are dwindling fast, with seemingly less than ten percent of industrial control systems using this as a current cybersecurity approach.

But even air gaps are not invulnerable. The well-known Stuxnet attack breached the Iranian nuclear program on an infected USB drive, issuing hardware commands from the inside and causing nuclear centrifuges to break down at Iran's nuclear plant Natanz.[35]

AIR GAP	DATA DIODE	FIREWALL
Strengths		
· Complete isolation of a network from the outside world	· One-way secure flow of information · 100% secure	· Facilitates regular and secure information sharing
Weaknesses		
· Not real time · Vulnerable to bad user behavior · No modern internet connection	· Can be perceived as expensive and complex to install · Vulnerable to physical tampering and bad user behavior	· Prone to bugs and mistakes · Vulnerable to software updates, hacks, bad user behavior and physical tampering

Table 2: **Air gap, data diode and firewall compared.** [36]

32 "Air-Gaps, Firewalls, and Data Diodes in Industrial Control Systems." White Paper. Nexor, May 2017. https://www.nexor.com/wp/wp-content/uploads/2017/05/Air-Gaps-Firewalls-and-Data-Diodes-in-Industrial-Control-Systems.pdf.

33 Scott, "Tactical Data Diodes in Industrial Automation and Control Systems."

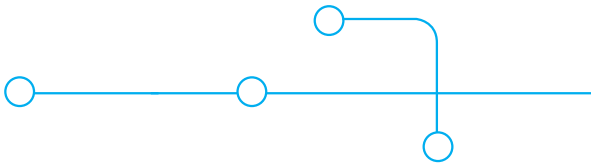
34 Ibid.

35 "The Enterprise Immune System." Dark Trace, n.d. https://www.darktrace.com/en/technology/. "Timeline: How Stuxnet Attacked a Nuclear Plant." BBC, n.d.

36 "Protecting Critical Assets and Production Environments." Fox-IT, September 2016. https://www.fox-it.com/datadiode/wp-content/uploads/sites/9/2016/10/Fox-DataDiode-Protecting-Critical-Assets-EN-2016.pdf.

Firewalls are pieces of software that manage the connections one network has with another. This approach has the potential to facilitate and regulate efficient and secure information sharing. However, its software-based foundation makes it inherently susceptible to a number of vulnerabilities, similar to other error-prone software. Lack of operating system updates, software vulnerabilities, backdoors, and misconfigurations leave networks exposed to threats.[37] Bugs, hacks and domain name server (DNS) tunneling constitute the most prevalent forms of attack on firewalls.[38]

A **data diode** has similar characteristics when compared to a firewall but approaches the same security problem using hardware. By physical design, data diodes only allow one-directional flow of information. In and of itself, it is one hundred percent secure because of this hardware design, which allows data to only flow in one direction.



However, data diodes are more complex to install and up until now have not experienced the same level of public awareness. This makes it difficult to integrate into existing systems.

It is important to note that the attack vectors change regularly. The most notable and recent shift is from exploiting software vulnerabilities to exploiting human vulnerabilities. As more attention is paid to creating secure software that is regularly updated and patched, perpetrators focus on the chance of human error, which continues to constitute a source of vulnerability. However, while data diodes only offer hardware solutions, they do prevent a large swatch of human errors which otherwise would be much more prevalent. As such, they provide better security even in the case of human error.

37 Scott, "Tactical Data Diodes in Industrial Automation and Control Systems."

38 "Air-Gaps, Firewalls, and Data Diodes in Industrial Control Systems."

5 – Data Diode Stakeholder Landscape

5.1 Use Case Environment

Although data diode technology has been around for many years,[39] its usage has been primarily confined to networks that require high-level security such as automated defense systems, transportation, industrial automation and control systems (IACS/SCADA), water and nuclear treatment facilities, and medical systems. In addition to high security environments, data diodes can help reduce risks in a variety of other commercial scenarios. To a limited extent, transmit-only data diodes have been used in protective monitoring, both physical (such as CCTV) and digital (such as network monitoring).[40] Transmit-only data diodes can also protect system integrity of certain back-office and oversight systems, such as voice or transaction recording, which are expected to be working near-constantly, for example, in a police station. A transmit-only data diode can segregate the source of the voice or transaction data and the recording systems and, as such, ensure that any regulatory matters can be investigated and complied with in confidence.[41]

Both configurations of data diodes can also provide business continuity. To prevent loss of data, companies perform regularly-scheduled backups. If not ensured the same level of protection, such duplication of, and connectivity between, live and backup systems introduce vulnerabilities that an attacker can exploit.

Vulnerabilities of primary systems get replicated into secondary systems, along with connectivity enabling exploitation. Receive-only data diodes enable a one-way data path from the live to the backup systems, reducing the opportunity for attack during data replication, ensuring the availability and integrity of data.[42]

The application of data diodes in automotive industry and airplanes (between flight control units and in-flight entertainment systems and wifi) is currently being explored. According to our interview respondents, sectors such as financial services, accounting, legal services, or small manufacturing plants can be made significantly more secure by using data diodes.

5.2 Vendors

Because data diode technology has so far been confined to national critical infrastructure and IACS/SCADA, the developers landscape has also remained limited. According to OPSWAT, there are only around 15 vendors of data diode technology around the world.[43] They range from large multinational companies such as BAE Systems and Boeing, that operate in a broad defense and security domain, to more cybersecurity specific firms such as Fox-IT and Owl Cyber Defense. The data diode technology that these companies market also varies depending on their certifications. Some carry higher Evaluation Assurance Level certifications (EAL-7), which measures the assurance requirements of an IT product of system, while others carry lower certifications, such as EAL-4 and EAL-2. Most owners and operators of national critical infrastructure are satisfied with EAL-4 certification.[44]

39 Fox-IT, Tieto security services, etc.

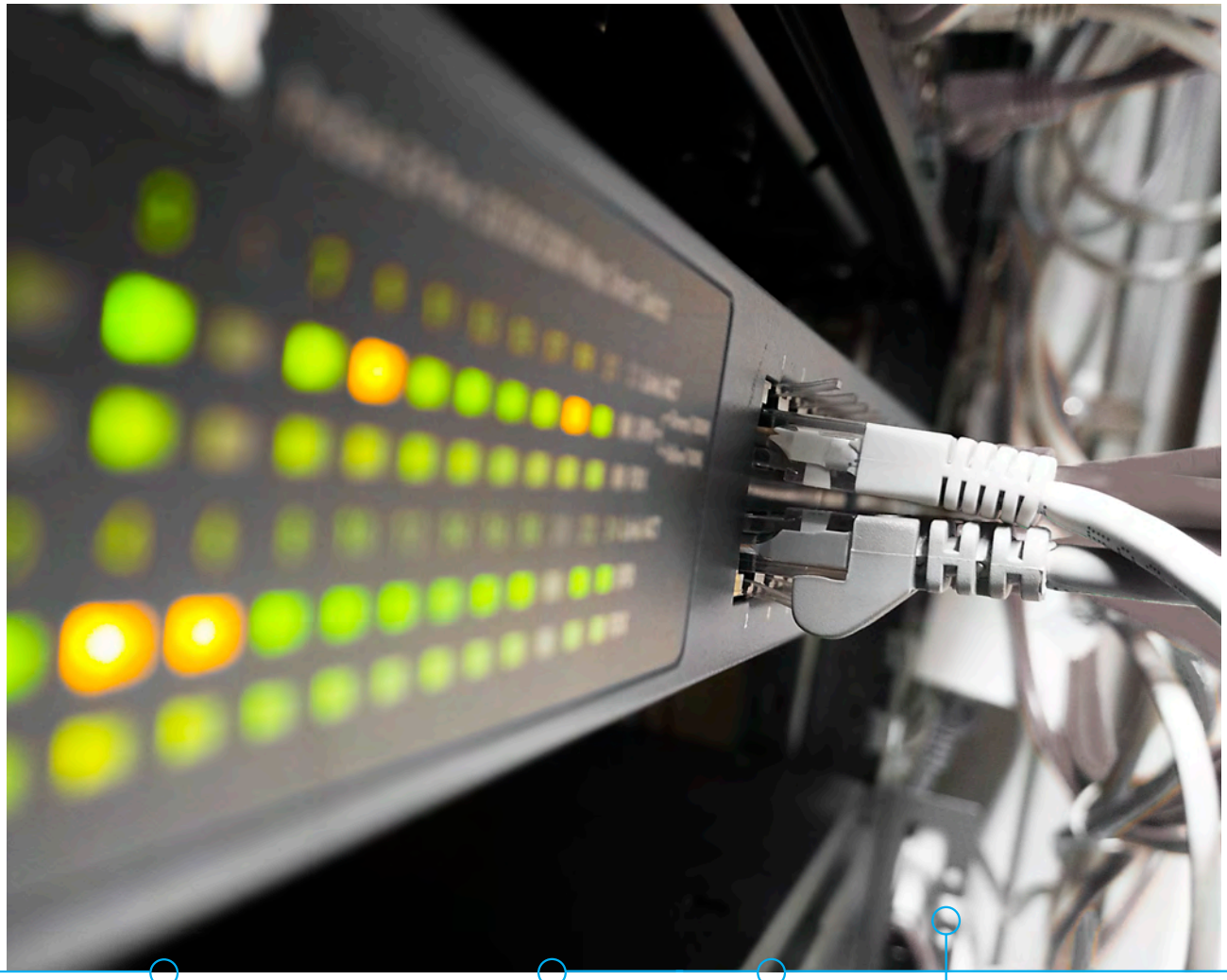
40 "Private Sector Cyber Resilience and the Role of Data Diodes." White Paper. NCC Group, April 25, 2016. https://www.nccgroup.trust/uk/our-research/private-sector-cyber-resilience-and-the-role-of-data-diodes/. 10

41 Ibid.11

42 Ibid.

43 "Data Diode Vendor Comparison Guide." OPSWAT, March 2017. https://info.opswat.com/data-diode-comparison.

44 Based on interview results



Data diodes are produced in a variety of countries including Israel, the UK, the US, the Netherlands, Denmark, Sweden, Germany, and Singapore. Data diodes can be measured by whether they offer optical or unidirectional software technology, which transfer protocol the hardware supports, the transfer rate of data, and the nature of input/output.

In recent years, the number of developers/vendors has increased and the market has broadened in scope. This is evident in the emergence of companies such as Compumatica, Deep Secure, Vado One Way Security, and Waterfall Security. There are even open source developers now in existence, such as DYODE.[45] In other words, the data diode market is growing hand in hand with its expanding market base.

5.3 Opportunities for Dutch Stakeholders

Despite the increasing importance of data diode technology, the Netherlands R&D position on data diodes remains quite small globally. Cybersecurity and IT company Fox-IT is the only Netherlands-based stakeholder which is successful in exporting its technology to more than 40 countries.[46] At the national level, only two companies advertise data diode technology as their main selling point, namely Fox-IT and Compumatica. French-based Thales, which also operates in the Netherlands, is marketing its ELIPS-SD diode.[47]

Although innovation appears to be on the rise, American, Israeli, and British companies continue to dominate most of the market. The underdeveloped nature of the data diode market provides ample opportunities for new entries.

Although its usage has been confined to critical national infrastructure so far, broader rollout can be expected. With more competition among the data diode vendors, prices will drop and industries such as airlines and automobiles will begin to seek out data diode vendors. By getting ahead of that curve, it would be possible for the Netherlands to have a head start on data diode production and offer up useful solutions.

45 "Dyode: A Low-Cost, DIY Data Diode for ICS." GitHub, October 7, 2017. https://github.com/wavestone-cdt/dyode.

46 Based on interview results

47 "New Thales Cybersecurity Solution for Industrial Networks." *Thales* (blog), September 30, 2015. https://www.thalesgroup.com/en/worldwide/security/press-release/new-thales-cybersecurity-solution-industrial-networks.

6 – New Developments in Data Diodes

The previous sections addressed the strengths and weaknesses of data diode technology and of the playing field. In addition to this, there are number of external factors that affect and exacerbate the development of the technology, its level of security and economic potential. In this chapter, we identified and examined economic (6.1), legal/regulatory (6.2), political (6.3) and technological (6.4) factors.

6.1 The Market Condition of Data Diodes

One of the main focus areas in the Netherlands' new Cybersecurity Agenda is to be at the forefront of digitally secure hardware and software.[48] With its intrinsic qualities and the currently available experience, data diodes could provide a relevant opportunity here. A more cost-effective version of a data diode could be on the way, especially given that the Dutch Cyber Security Agenda has outlined a 95 million EUR figure for structural funding, that other countries are discussing data diode technology in their technological development papers, and that use cases are expanding.

According to interview respondents, the possibility of a more cost-effective data diode is a very likely one, particularly if the usage of FPGA chips – which allow for more flexible programming of proxy servers – increases as alternatives for full proxy servers. That shift would mean that the cost of a proxy server would correspondingly decrease, as would the overall expense of a full data diode.[49]

Several interviewees pointed out that one of the main reasons for the continued high cost of data diodes is the market condition; namely that it is dominated by the defense industry, where price is not nearly as important as efficiency. As data diode technology comes increasingly into play for commercial industries, this market condition will become less important.[50]

6.2 Compliance

Legal requirements, increasing cyber investments, and the still dormant security concerns would give incentives to a growing market. For instance, other countries have noted the important role that data diodes play. The US Department of Homeland Security (DHS) has best practices which stipulate that companies should isolate high secure networks from insecure ones, as well as using network segmentation to restrict and isolate communication pathways. Explicitly, they also state that "if one-way communication can accomplish a task, use optical separation ("data diode")."[51] The British-based National Cyber Security Centre also suggests the use of data diodes, stating that "when sending logs across trust boundaries, they should be sent across a one-way flow control (e.g. UDP or a data diode)."[52] While compliance is not prescribed nor required in Europe as of yet, organizations including the French Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)[53] promote the use of data diodes.

48 "Cyber Security Assessment Netherlands 2018."

49 Based on interview results

50 Based on interview results

51 Coleman, Scott. "Implementing DHS Best Practices to Secure Industrial Control Systems." *Owl Cyber Defense* (blog), May 25, 2018. https://www.owlcyberdefense.com/blog/2018/5/25/implementing-dhs-best-practices.

52 "Introduction to Logging for Security Purposes." National Cyber Security Centre, July 9, 2018. https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.

53 "Agence Nationale de la Sécurité des Systèmes d'Information," n.d. https://www.ssi.gouv.fr/en/.

Furthermore, the Dutch Cyber Security Agenda points to agreements that will be set on compliance and standards for cybersecurity.[54] These kinds of standards have driven the development and further innovation of data diode technology in the United States, and may do the same in Europe. In the United States, compliance is what drove the growth of the data diode technology market as segregation of networks was mandated. That same trend is on the rise in the Middle East as well.[55] Currently, the European Parliament is debating the prospect of these very measures being Europeanized.[56] Because compliance measures are what drove the American market to grow so quickly, it follows that compliance measures may also encourage data diode technology dissemination in Europe. With more stringent compliance measures, companies will be required to buy data diodes, and correspondingly will demand lower cost alternatives. This presents an opportunity for data diode producers to come up with lower-cost alternatives, allowing clients in subcritical and mainstream sectors to adopt this hardware approach.

In 2017, the Dutch Data Protection Authority reported that data leaks increased by over seventy percent compared to the previous year, from 5,849 to 10,009.[57] Diodes can contribute to an intrinsically more secure cybersecurity landscape as they function as one of the only methods that effectively prevent data leakages and protect high confidentiality data from certain forms of cyber attacks. Data diodes also play a role in segmenting possible data leakages because high secure networks would no longer be accessible for hackers. Due to their high cost, it is unlikely that many companies other than the ones mandated to do so (i.e., Type A Critical Infrastructure Companies) will implement these measures.

This is because the range of clients is restricted to the defense industry and national critical infrastructure, which are willing to pay the current market price. With a more diverse range of clients, some may neither be willing nor be able to pay the current market price, encouraging the introduction of more cost-effective options. To bring down the cost, it may be useful to consider promoting and encouraging more entrepreneurship and collaboration, and to operate more knowledge-sharing ventures in this particular field of hardware security.

6.3 Export and Innovation Possibilities

If the Netherlands could become a source for data diodes, it could be very useful to export to other European countries; especially considering the current European Parliament debate about standardizations and certifications.[58] Tenders already exist that offer collaboration opportunities with the US Department of Homeland Security.[59] Data diode technology is an opportunity for Dutch producers such as Fox-IT and Compumatica to take advantage of their market position by collaborating with foreign partners such as the US Department of Homeland Security and large firms such as Siemens, General Dynamics, as well as potential new players.

The new Dutch Cyber Security Agenda promotes both privacy and hardware security in order to prevent cybercrime.[60] Collaboration between organizations such as the NCSRA, dcypher, KennisNet, the National Cyber Security Centrum, the Digital Trust Center, the Dutch Digital Delta, and the National Detection Network would be useful to create a research and development hub. Furthermore, the Netherlands Organization for Scientific Research (NWO) could serve as a funding mechanism to encourage research into this particular field.[61]

54 NCTV, "National Cyber Security Agenda: A cyber secure Netherlands." Ministry of Justice and Security, April 22, 2018. https://www.enisa.europa.eu/news/member-states/CSAgenda_EN.pdf.

55 "Private Sector Cyber Resilience and the Role of Data Diodes."

56 Stupp, Catherine. "Plan for EU Cybersecurity Certification Receives Parliament Approval." *Euractiv*, July 10, 2018. https://www.euractiv.com/section/cybersecurity/news/plan-for-eu-cybersecurity-certification-receives-parliament-approval/.

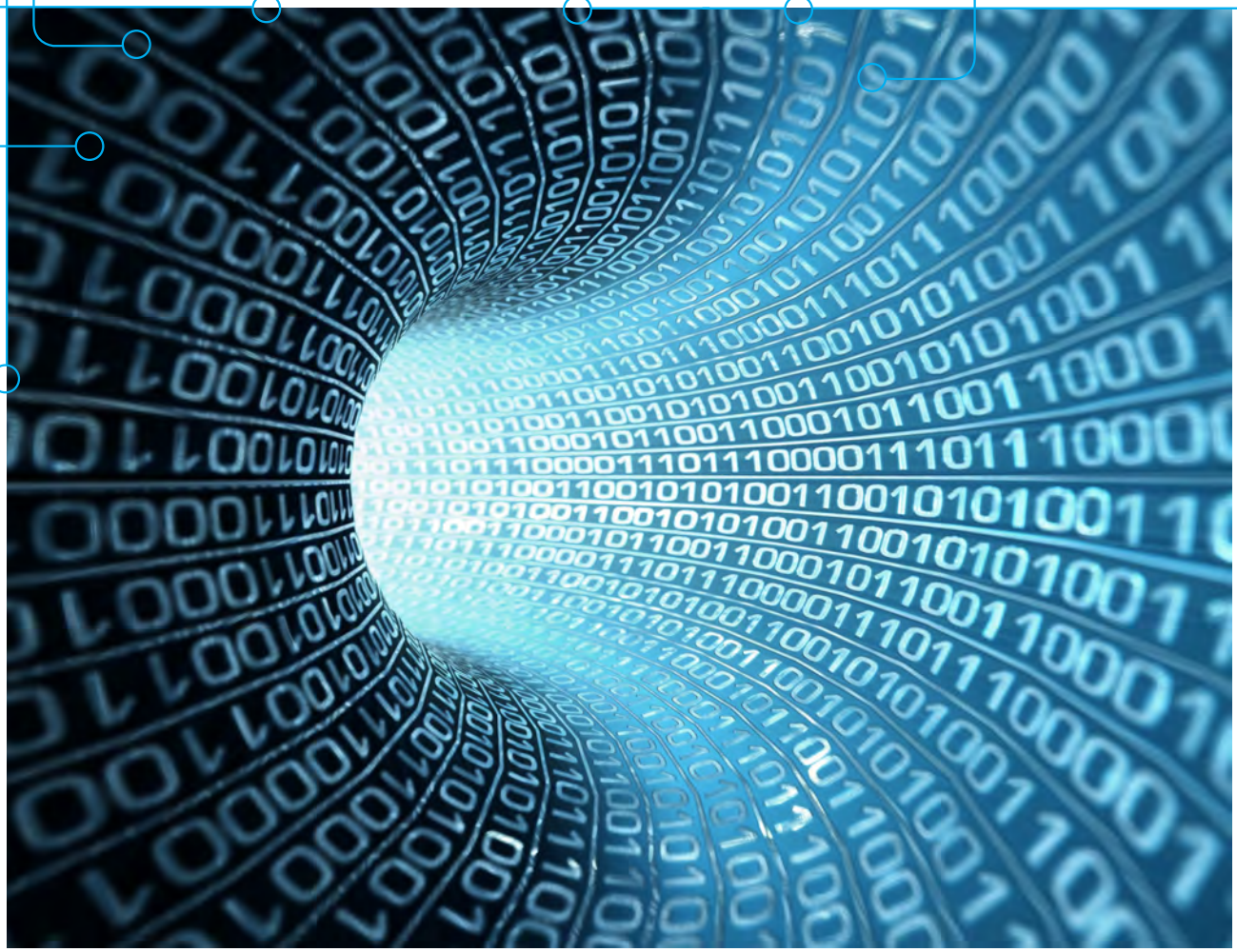
57 "Cyber Security Assessment Netherlands 2018." 30

58 "Draft Agendas: European Parliament Committee on Industry, Research and Energy." European Parliament, n.d. http://www.europarl.europa.eu/committees/en/itre/draft-agendas.html.

59 "Announcement Bilateral Call for Proposals Cyber Security." Ministry of Justice and Security, May 18, 2017. https://www.ncsc.nl/english/current-topics/news/dhs-st-cyber-security-division-netherlands-counterparts-announce-bilateral-funding-call.html.

60 NCTV, "National Cyber Security Agenda: A Cyber Secure Netherlands."

61 "Announcement Bilateral Call for Proposals Cyber Security."



The question for many industries remains, why consider using data diodes in the first place? The answer is that they offer complete protection from internet-based threats. Rather than constantly worrying about the vulnerabilities in firewall software, data diodes assuage some of the risk inherent in being connected to the internet. Furthermore, data diodes can provide protection for legacy systems. Eighty-five percent of factories in the Netherlands are older than ten years. For many of these factories, it is challenging to adapt their legacy systems to current cybersecurity solutions.[62] Data diodes can protect a factory's operations without leaving it vulnerable during an update procedure for the operational technology (OT) network, whether hardware or software.

6.4 New Fields and the Internet of Things

Consider also the industries of smart cars and airlines. Companies like Tesla have already been hacked, which showcases the weaknesses of the smart automotive sector. Airlines are looking into segregating wifi and entertainment systems from the cockpit and airplane control systems. These types of future developments show that data diodes will become more commercially used in the future, and their implementation therefore more important to invest in.

62 Based on interview results

In particular, the emergence of the Internet of Things (IoT) portends the increase in security risks. As collection and flows of data soar, so too do risks to data privacy and security. Moreover, sensitive data no longer only travels through, or is maintained on, government and infrastructure channels. Hospitals and cars now operate digital technologies that can be manipulated. As these technological developments continue to grow, transmit-only data diodes would allow networks transmitting sensitive data to feel confident in the knowledge that their data remains secure.

6.5 Open Source vs. Closed Source

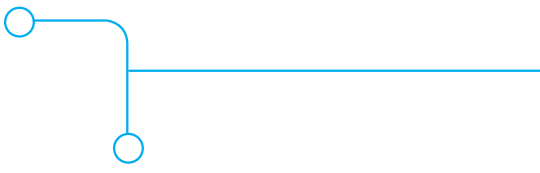
According to interview respondents, open source developments in the data diode market are very likely. However, many also believe these developments are not pertinent given the highly secure nature of the defense industry. In fact, many diagrams for how to build a data diode at home are already publicly available. Many protocols that guide the general communication are also available over open source forums. However, there is a vast diversity of protocols that often require specific data diode structuring. This means that oftentimes data diodes must be crafted to respond to unique protocols. As they are tailored to a specific environment or one-time use only, their source code is not necessarily opened up.

Despite these difficulties, open-source software is becoming more popular in cybersecurity. This is because open source provides more trust as the original code itself is public. Moreover, by publishing the code more people can contribute and add more features to it. Additionally, making code open source gives it the ability to outlive a company should it go bankrupt. However, according to interview results, if open and closed source data diodes are offered in the same price range, clients are more likely to opt for a closed source version due to brand recognition.

At the HSD Roundtable, stakeholders discussed the viability of open source data diodes and whether or not it was feasible to make this technology open source without compromising security. Products such as OpenVPN-NL were brought up as an example of a security-based software that has been developed on an open-source basis, paired with consistent updates to minimize the possibility of hacking.[63]

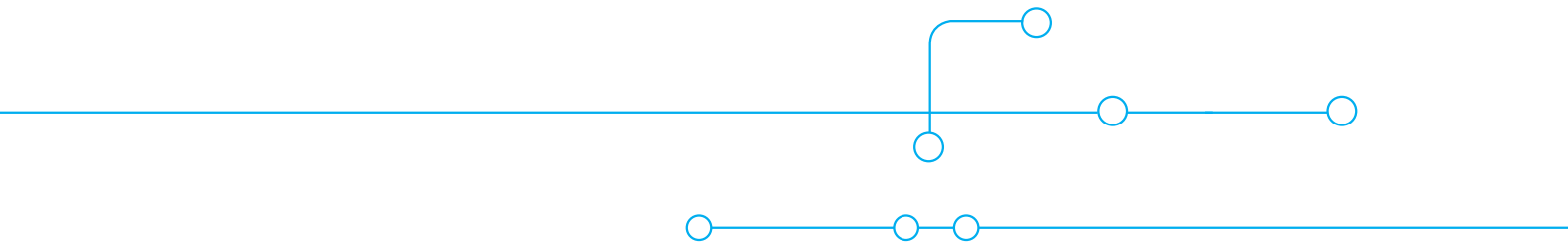
This addresses one of the concerns of open source data diodes, namely that consistent patching and updating of the protocol-related software behind proxy servers is necessary in order to mitigate the risks inherent in posting this technology online. Perhaps the most important takeaway here is that patching of open source data diode software is not the problem, but instead it is the diversity of environments in which data diodes need to be integrated. How will data diodes be built to handle the wide range of different settings and protocol use?

Notably, many discussants brought up the point that low-end open source data diodes were a possibility; for example, to stream data and videos securely and maintain secure Twitter and Facebook feeds, rather than for national security and intelligence agencies. In other words, while open source data diodes constitute a potential innovation for lower risk networks, closed source data diodes are momentarily the norm for classified governmental networks and applications. In short, the discussion about which is safer, open source (scrutiny) or closed source (presumably updated), is still very much open without a clear winner. There are examples of open source software with a quick patch cycle, as well as examples to the contrary.



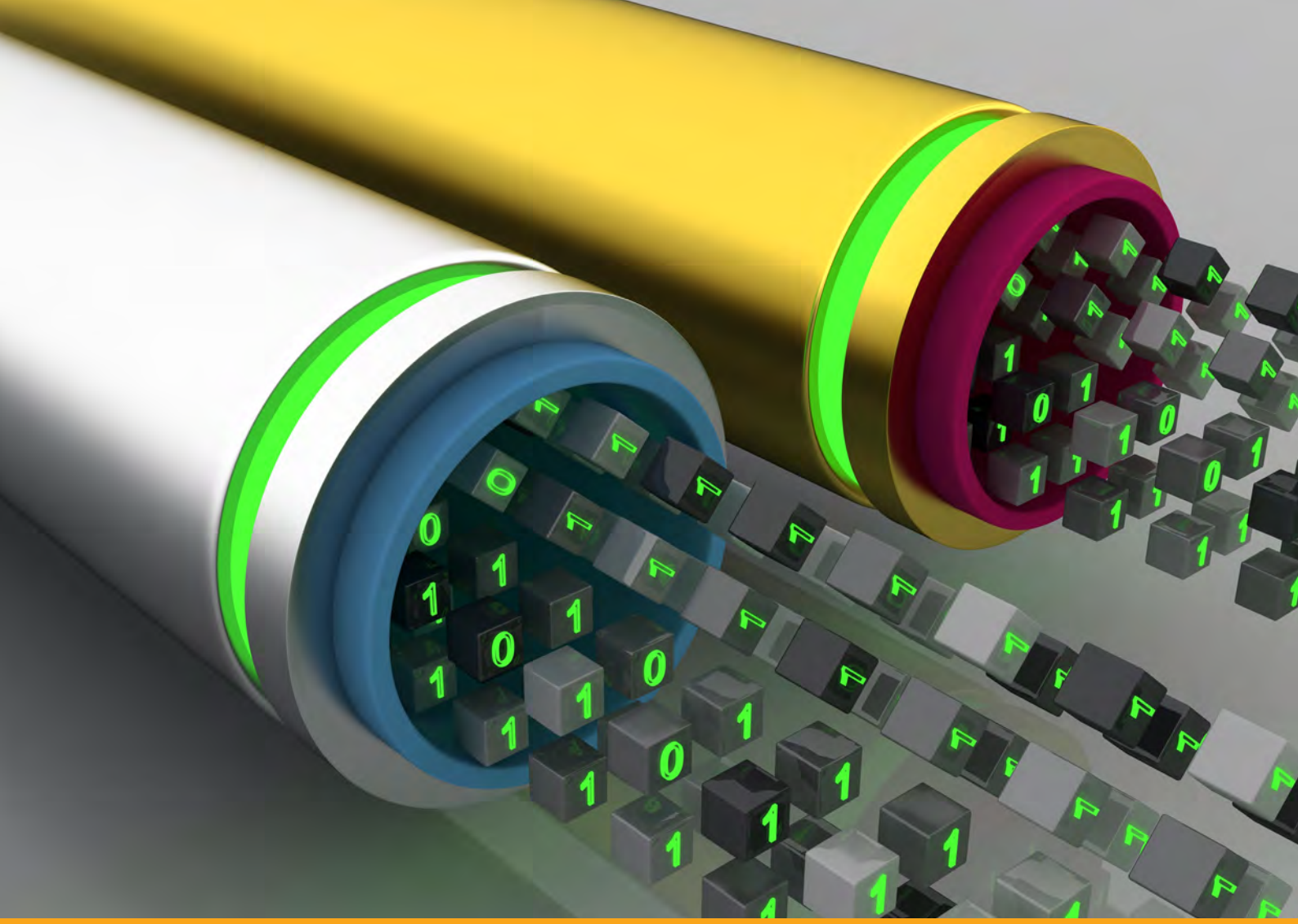
63 OpenVPN-NL, for example, patches their software 24 hours after incidents are reported, leaving little leeway for malware and entry points for attacks.

Beyond the open and closed source question, however, the consequences of widespread usage of data diodes must be investigated, and their weaknesses must be clear. Price and the market conditions of the defense and security industry, for example, are factors that many stakeholders and interviewees point to as the reason why data diodes are not standardized technology for every industry. However, according to interviews, a data diode could be built using open source technology for as little as 1,000 EUR.[64] This extreme difference in market price versus open source technology-based price has to do with how data diodes are perceived in the market, i.e. as expensive niche products. An additional cost is certification. The certification of a cybersecurity product by the French Cybersecurity Agency can cost anywhere from twenty to thirty thousand euros.[65] At current demand levels, certification is a significant factor that drives up prices.



64 Based on interview results

65 Based on interview results



7 – Conclusions

Data diode technology is not the new kid on the block. With technology development dating back to the latter part of the 20th century, practical implementation of data diodes goes back to the beginning of this century. Historically, its implementation was limited to the military and defense sectors. Industrial control systems constitute the second (emerging) market. However, in the past two to three years, data diode technology has been receiving increased attention.

One of the most attractive components is its physical dimension in providing security. In a world where there are more and more networks exposed to vulnerability, data diodes provide a valuable potential addition to the current cybersecurity toolbox.

For now, attention has been focused primarily on the high-risk spectrum: the functioning of critical infrastructure and the protection of classified information systems. Any sort of disruption or breach within this spectrum could lead to significant problems on a national level, thus affecting the national security of a country. As such, governments have upped their involvement, establishing legislation and guidelines in order to improve the overall security level of critical infrastructure (generally operated by private sector actors) and sensitive information assets (both in the public and private domain). Increasingly, data diodes are mentioned as a possible tool to improve security levels, especially when it comes to remote access policies and surface area limitations. However, the costs of acquisition and implementation of current data diode technology are steep. At the same time, such costs are lower than the potential damage that a breach or disruption would cause.

Open source developments and an increasing competitive environment in the low-end segment might cause prices to drop. As of yet, open source developments of both hardware and software related to data diodes have limited price effects. The occurrence of manufacturers in the lesser grade sector – with lower or no specific certification levels – is increasing and providing downward price incentives. According to interview respondents, more cost-effective versions of data diode technology are expected to arrive the coming two years.

The focus on subcritical and mainstream processes or assets (i.e., where the costs of disruption would affect the national interests to a much lesser extent) is not yet prevalent. There are several potential use cases in this domain that might warrant more attention. Some of these may be caused by stricter regulation related to the protection of personal data and compliance with information laws. Others are the result of the sheer value of data that companies are holding, such as intellectual property or data collections (big data).

Data diodes continue to be perceived as niche and expensive. Potential customers lack familiarity with this technology, the relevance of its use, and the price range available. This obstructs the potential rollout of data diodes. As put by one of the interviewees: “It is difficult to sell tires to people who do not know what they are.” Regarding costs of acquisition and maintenance, potential customers seem unaware of the extent to which long term low operating costs justify high initial costs. By means of questionnaires, reports, and awareness raising campaigns, vendors of this technology are trying to change existing perceptions. From the vendor’s perspective, setting new European standards constitutes a way forward.

Overall, data diode technology can be a very valuable addition to a broader cybersecurity toolbox, part of a comprehensive security posture that should also involve tools such as monitoring and the ability to rapidly respond to threats that materialize. Its hardware-based characteristics provide it with a unique protection model within this broader toolbox.

8 – Recommendations

Based on the analysis in this paper, the following *objectives* should be envisioned:

- Defending networks against external threats in general. Protecting the confidentiality, integrity, and availability of a network and, in particular, the data that resides on it.

- Providing cybersecurity and network connectivity at the same time: Ensuring that sensitive, high-value networks remain protected and, at the same time, open to providing and incorporating data flows to authorized users on demand.

Based on our analysis, the following recommendations can be made:

- Data diodes are currently perceived as niche and expensive. The rollout of this technology is further obstructed by the fact that potential customers lack familiarity with the technology as such, the relevance of its use, and the price range available. By means of surveys, reports and awareness-raising campaigns, data diode vendors could help address the current lack of knowledge, increase the awareness of the potential of data diodes, and change existing perceptions.

- Many companies do not possess ICT skills in general, and the specialized knowledge and skills to install data diodes in particular. Attention should be paid to ensuring that data diode installation trainings are available online and/or form part of computer science and information technology curricula.

- Although the usage of data diodes has been primarily confined to networks that require high-level security, applicability of this technology goes beyond the realm of critical national infrastructure and IACS/SCADA. Non-critical sectors such as aviation, automotive industry, financial services, health care services, accounting, legal services, or small manufacturing plants would also benefit from the implementation of data diodes. It is equally important to promote the adoption of data diode technology in legacy systems (such as factories older than ten years and elections). Attack vectors change regularly. To control for multiple attack vectors, the most comprehensive solution appears to be the one that utilizes one or more of the available security solutions – a combination of an air gap, data diode, and/or firewall.

- Experience with the development and marketing of data diode technology provides an opportunity for Dutch stakeholders to place themselves at the forefront of marketing digitally secure hardware and software in general, and of data diode technology in particular.

- The data diode market is growing hand-in-hand with its expanding market base. With more competition among the data diode vendors, prices are expected to drop and industries such as airlines and automobiles are expected to begin to seek out data diode vendors. Dutch companies should keep abreast of these developments, and get ahead of the curve by coming up with lower-cost data diode solutions that will cater to the demands of potential clients in subcritical and mainstream sectors.

- Setting new European standards constitutes a way forward. Following the example of the United States, introducing compliance requirements at the national and/or European level would likely enhance the knowledge, use, and understanding of this technology outside of national critical infrastructure organizations. With more stringent compliance measures, companies will be required to implement these measures, and correspondingly can demand lower cost data diode solutions. When costs drop, it will also be more likely that those companies that are not mandated to implement data diodes will nevertheless consider doing so.

- To bring down the costs, more entrepreneurship and collaboration should be promoted and encouraged, and more knowledge-sharing ventures should be operated in this particular field of hardware security, as is currently occurring in open-source diode efforts. Communities of practice and knowledge centers that support enterprises in securing their digital operations – such as the Netherlands' Digital Trust Centre – should consider data diodes as part of the cybersecurity toolbox.

- In light of the current debate in the European Parliament regarding standardizations and certifications, Dutch companies could take advantage of their frontrunning market position and start exporting data diodes to other European countries. Opportunities for collaboration with foreign partners such as the US Department of Homeland Security, and multinational firms, as well as potential new players, should be explored.

- To prevent cybercrime, the new Dutch Cyber Security Agenda promotes both privacy and hardware security. Collaboration between organizations and networks such as dcypher, KennisNet, the National Cyber Security Centrum, the Digital Trust Center, the Dutch Digital Delta, and the National Detection Network would be useful to create a research and development hub. The Netherlands Organization for Scientific Research (NWO) could serve as a funding mechanism to encourage research in this particular field and with a specific focus of integration in new application domains.

- The consequences of widespread usage of data diodes must be investigated, and their weaknesses must be clear.

Annexes

Annex 1 – Interview Questionnaire

Data Diode Market

1 How large would you consider the data diode market to be (in units)?
2 What is your experience of marketing data diodes in the Netherlands thus far?
3 In your opinion, what are future avenues/ approaches, which could be pursued to make data diode technology more affordable?
4 Do you see the development of the market moving in that direction?
5 Have you worked with foreign partners or do you know of such opportunities?
6 Do you feel that the Netherlands has enough stakeholders to turn data diode technology into an export product? If so, what approach do you feel is most appropriate?
7 Who do you compete with?
8 What are your unique selling points/propositions?

Open source data diodes

9 How do you perceive the likelihood of open source developments?
10 Do you know of any companies that use open source data diodes?

Costs of data diode technology

11 How do various factors contribute to the overall costs (production, materials, software, maintenance)?
12 How would it be possible to lower the costs in that case (i.e, where are the biggest costs gains to be made)?

Customer base

13 Who are targeted customers? Is it only high-end?
14 If so, is there no market in more mainstream applications (i.e., IoT)?
15 If there are also other segments, what types of processes or products would benefit from data diodes (concrete examples)?
16 Are they universally applicable? What are their particular strengths, what are their weaknesses compared to other cybersecurity tools?
17 Are there factors beyond your control that hinder or could stimulate broader rollout?
18 As far you know, do vital parties like using data diodes and why?
19 In your opinion, why would sub-vital parties (i.e. companies who are not in Industrial Control and Automation Networks or Critical National Infrastructure) want to use diodes?
20 Do you see an increased awareness of the potential of DD?

Annex 2 – List of Interviewees

Name	Affiliation
Maria Douich Scott Coleman	OWL Cyber Defense OWL Cyber Defense
Andres Gonzales Guilarte	Siemens Data Capture Unit
Petra van Schayik	Compumatica
Peter Geijtenbeek	Fox-IT
Arnaud Soullie	Wavestone
Jaya Balou	KPN

Bibliography

Admin. "One-Way Network Security; How to Recognize a True Data Diode?" *Fox-IT* (blog), June 18, 2018. https://www.fox-it.com/datadiode/2018/06/18/one-way-network-security-recognize-true-data-diode/.

"Agence Nationale de La Securite Des Systemes d'Information," n.d. https://www.ssi.gouv.fr/en/.

"Air-Gaps, Firewalls, and Data Diodes in Industrial Control Systems." White Paper. Nexor, May 2017. https://www.nexor.com/wp/wp-content/uploads/2017/05/Air-Gaps-Firewalls-and-Data-Diodes-in-Industrial-Control-Systems.pdf.

"Announcement Bilateral Call for Proposals Cyber Security." Ministry of Justice and Security, May 18, 2017. https://www.ncsc.nl/english/current-topics/news/dhs-st-cyber-security-division-netherlands-counterparts-announce-bilateral-funding-call.html.

Barry, Courtney. "Data Diodes for Cyber Security." *TechSurveillance Magazine*, March 2012. http://courtneybarry.com/Images/TS_Data_Diodes.pdf.

Bordel, Borja, Ramon Alcarria, Diego Sanchez-de-Rivera, and Tomas Robles. "Protecting Industry 4.0 Systems Against the Malicious Effects of Cyber-Physical Attacks. Ubiquitous Computing and Ambient Intelligence." *UCAmI 2017. Lecture Notes in Computer Science* 10586 (October 7, 2017): 161–71. https://doi.org/10.1007/978-3-319-67585-5_17.

Brewster, Thomas. "NotPetya Ransomware Hackers 'Took Down Ukraine Power Grid.'" *Forbes*, July 3, 2017.

Carter, Candice. "Critical Infrastructure and Cyber Security." Incapsula Blog, October 30, 2017. https://www.incapsula.com/blog/critical-infrastructure-cyber-security.html.

Coleman, Scott. "Implementing DHS Best Practices to Secure Industrial Control Systems." *Owl Cyber Defense* (blog), May 25, 2018. https://www.owlcyberdefense.com/blog/2018/5/25/implementing-dhs-best-practices.

"Cyber Security Assessment Netherlands 2018." Ministry of Justice and Security, August 7, 2018. https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html.

"Data Diode Vendor Comparison Guide." OPSWAT, March 2017. https://info.opswat.com/data-diode-comparison.

"Digital Trust Center," n.d. https://www.digitaltrustcenter.nl/.

"Draft Agendas: European Parliament Committee on Industry, Research and Energy." European Parliament, n.d. http://www.europarl.europa.eu/committees/en/itre/draft-agendas.html.

"Dyode: A Low-Cost, DIY Data Diode for ICS." GitHub, October 7, 2017. https://github.com/wavestone-cdt/dyode.

"Fox-IT Data Diodes One-Way Traffic Keeps Secrets Safe." Fox-IT, 2016. https://www.fox-it.com/datadiode/wp-content/uploads/sites/9/2016/07/Fox-DataDiode-One-Way-Traffic-keeps-Secrets-Secret-023-101-EN.pdf.

"Gartner Says AI Technologies Will Be in Almost Every New Software Product by 2020." Gartner, July 18, 2017. https://www.gartner.com/en/newsroom/press-releases/2017-07-18-gartner-says-ai-technologies-will-be-in-almost-every-new-software-product-by-2020.

Gedrojc, Bartek. "Fort Fox Hardware Data Diode: Security Target: Common Criteria FFHDD – EAL7+." White Paper. Fox-IT, June 3, 2010.

Gonzalez Guilarte, Andres. Interview with Andres Gonzalez Guilarte. Phone, November 1, 2018.

NCTV, National Cyber Security Agenda: A cyber secure Netherlands, Ministry of Justice and Security, April. https://www.enisa.europa.eu/news/member-states/CSAgenda_EN.pdf.

"Introduction to Logging for Security Purposes." National Cyber Security Centre, July 9, 2018. https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.

"Kamerbrief over Innovatiebeleid En de Bevordering van Innovatie: Naar Missiegedreven Innovatiebeleid Met Impact." Ministerie van Economische Zaken en Klimaat, July 13, 2018. https://www.rijksoverheid.nl/documenten/kamerstukken/2018/07/13/kamerbrief-naar-missiegedreven-innovatiebeleid-met-impact.

Koerner, Brendan. “Inside the Cyberattack That Shocked the US Government.” *Wired*, October 23, 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

Menoher, Jeffrey. “Not All Data Diodes Are Equal.” White Paper. Owl Computing Technologies, September 6, 2013. http://www.scadahackr.com/library/Documents/White_Papers/Owl%20-%20All%20Data%20Diodes%20Are%20Not%20Equal.pdf.

“New Thales Cybersecurity Solution for Industrial Networks.” *Thales* (blog), September 30, 2015. https://www.thalesgroup.com/en/worldwide/security/press-release/new-thales-cybersecurity-solution-industrial-networks.

Okhravi, Hamed, and Frederick Sheldon. “Data Diodes in Support of Trustworthy Cyber Infrastructure.” *CSIIRW ’10 Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, no. 23 (April 21, 2013). https://doi.org/10.1145/1852666.1852692.

“Private Sector Cyber Resilience and the Role of Data Diodes.” White Paper. NCC Group, April 25, 2016. https://www.nccgroup.trust/uk/our-research/private-sector-cyber-resilience-and-the-role-of-data-diodes/.

“Protecting Critical Assets and Production Environments.” Fox-IT, September 2016. https://www.fox-it.com/datadiode/wp-content/uploads/sites/9/2016/10/Fox-DataDiode-Protecting-Critical-Assets-EN-2016.pdf.

Robbins, Colin. “Can You Trust a $1612 Data Diode?” *CyberMatters* (blog), March 12, 2013. https://cybermatters.info/2013/03/12/can-you-trust-your-1612-diode/.

Schiffer, Alex. “How a Fish Tank Helped Hack a Casino.” *The Washington Post*, July 21, 2017. https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?noredirect=on&utm_term=.303ae5e989ad.

Scott, Austin. “Tactical Data Diodes in Industrial Automation and Control Systems.” SANS Institute InfoSec Reading Room, May 18, 2015. https://www.sans.org/reading-room/whitepapers/firewalls/tactical-data-diodes-industrial-automation-control-systems-36057.

Stupp, Catherine. “Plan for EU Cybersecurity Certification Receives Parliament Approval.” *Euractiv*, July 10, 2018. https://www.euractiv.com/section/cybersecurity/news/plan-for-eu-cybersecurity-certification-receives-parliament-approval/.

Teepe, Wouter, and Colin Robbins. “Protecting Confidential Information Using Data Diodes.” White Paper. Fox-IT, July 2014. https://www.fox-it.com/datadiode/wp-content/uploads/sites/9/2015/02/Fox-DataDiode-Protecting-confidential-information-using-data-diodes-EN1.pdf.

“The Common Criteria.” Common Criteria Portal. Accessed January 21, 2019. https://www.commoncriteriaportal.org.

“The Enterprise Immune System.” Dark Trace, n.d. https://www.darktrace.com/en/technology/.

“The National Cyber Security Research Agenda (NCSRA-III).” dcypher, June 5, 2018. https://www.dcypher.nl/sites/default/files/uploads/documents/NCSRA-III_0.pdf.

“Timeline: How Stuxnet Attacked a Nuclear Plant.” *BBC*, n.d. https://www.bbc.com/timelines/zc6fbk7.

Zetter, Kim. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.” *Wired*, March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Understanding the Strategic and Technical Significance of Technology for Security. The Case of Data Diodes for Cybersecurity @2019, The Hague Centre for Strategic Studies (HCSS) and The Hague Security Delta

A publication from
The Hague Security Delta (HSD)
Wilhelmina van Pruijsenweg 104
2595 AN Den Haag
T + 31 (0)70 204 5180
Info@thehaguesecuritydelta.com
www.thehaguesecuritydelta.com
@HSD_NL

Authors
Katarina Kertysova, Erik Frinking & Gabriella Gricius

Reviewer(s)
HSD Office Management Team

Design
Studio Maartje de Sonnaville by the design of
Studio Koelewijn Brügenwirth

Print
Drukkerij Edauw + Johannissen

This study was commissioned by the Hague Security Delta (HSD). The information and views set out in this study are those of the authors and do not necessarily reflect the official opinion of HSD. HSD does not guarantee the accuracy of the data included in this study. Neither HSD nor any person acting on behalf of HSD may be held responsible for the use which may be made of the information contained therein.

Together we Secure the Future

www.thehaguesecuritydelta.com