**Cybersecurity Case Study: Ransomware in the Netherlands (July 2022)**

**1.0 Introduction**

I choose the Netherlands for this case study as my family is originally from the Netherlands, specifically the southern region Eindhoven, and as such it’s an area of interest. Fascinatingly, Eindhoven is actually the tech hub of Holland, by comparison though the country as a whole is ranked third of the European tech hubs, with Germany and London in top positions (startup places, 2022). The High Tech Campus Eindhoven, sometimes referred to as the smartest square kilometer in Europe, boasts more than 140 companies and institutions, comprising of over 10,000 product developers, researchers and entrepreneurs and an estimated 85 nationalities. The Netherlands is in fact Europe’s most wired country and is the second most wired country in the world. Interestingly, 98 percent of every home having a fast broadband connection (80 Mbps), the first being Singapore (digital-strategy.ec.europa.eu, 2021).

Another reason for choosing the Netherlands was the country being one of Europe's top hubs for cybersecurity. Their National Cyber Security Centre (NCSC) is the main information hub and the centre of competence for countrywide cyber security. The NCSC promotes collaboration between the government and industry to enhance Dutch society's digital resilience. Many foreign security agencies, including Europol and NATO, have built their offices in the Netherlands, attracted by the strong technical ecosystem and good digital infrastructure (IT & Tech, 2022).

The Netherlands is the European leader in logistics and distribution operations. Coca-Cola, IBM, Samsung, TEVA and Tommy Hilfiger have all chosen the Netherlands as their logistics and distribution gateway to Europe. Impressively, 170 million consumers can be reached within 24 hours from Rotterdam or Amsterdam, making the Netherlands an ideal entry point into the European market. Interestingly, in the IT sector, 60% of Forbes 2000 businesses have already established operations in Holland, it is a hotspot for leading IT and communication companies (Share 4PL, 2021).

**2.0 Cybercrime Focus: Ransomware**

The cybercrime chosen for this presentation is one with a significant global presence, Ransomware. Ransomware is a type of malware or malicious software illegally infiltrated to prevent access to files, networks or systems, holding data ransom to be released only after a payment has been made (Federal Bureau of Investigation, 2021). Ransomware was the third most utilised technique for cyberattacks in 2021 globally and in the first half of 2021 there were 304.7 million ransomware attacks worldwide, up 151% above 2020.

Increasingly, ransomware in particular is being used to target government sectors and countries accross Europe. According to the European Union (EU) Agency for Cybersecurity (ENISA) the top five sectors affected are; public administration/government, digital service providers, general public, healthcare/medical, and finance/banking. According to data cited by the EU Agency for Cybersecurity, the average ransom payment increased from €71,000 in 2019 to €150,000 in 2020, and the largest ransomware demand increased from €13 million in 2019 to €62 million in 2021. Global ransomware losses are predicted to reach €18 billion in 2021, which is 57 times more than in 2015. In the second quarter of 2021, the average downtime for organizations that were attacked was 23 days and a corporate ransomware assault happened every 11 seconds or so in 2021 (www.europarl.europa.eu, 2022).

The Netherlands hasbeen very efficient at limiting the effect of ransomware attacks, facing some of the lowest ransomware threats in Europe with only 0.01% of computers facing this threat (The EE, 2020). However, since 2020, COVID-19 has compelled businesses to turn to digital transformation, and the last few years have seen cyberattacks reach an industrial scale.  According to the NL Times (2022), the Netherlands is facing a greater cyber security danger than Dutch businesses and organizations can withstand. In 2021 companies in the Netherlands paid over an average of $2 million in ransom to cybercriminals and that number is set to increase in 2022.

**3.0 Netherlands Dealing With Cybercrime**

The Dutch police in collaboration with IT security companies have taken a stand against ransomware, they have launched the online campaign ‘No More Ransom’ in order to counter the influx of ransomware attacks. This platform contains free decryption codes for many different types of ransomware (Europol, 2021). The Dutch government urge anyone who falls victim to ransomware attacks to first check this platform before paying cybercriminals. The police further advise both citizens and corporations not to pay ransomware, as doing so enables such criminal business models to remain in place.

It’s important to note that in most cases, even when ransom sums are paid, the malware is not completely removed, which can result in re-encryption of files at a later stage. The ‘No More Ransom’ platform began as a police initiative and has since grown into a international network, supported by institutions including; Kaspersky, Mcafee, Amazon and Europol’s European Cybercrime centre. Since its inception in July 2016, over 2.5 million people worldwide have consulted the platform (Nomoreransom.org, 2019).

**4.0 Global Legal and Regulatory Environment**

Today many international organizations including; the Organisation of American States (OAS), the EU, the Association of The Southeast Asian Nations (ASEAN), Group of 20 (G20), and the United Nations General Assembly’s First Committee on Disarmament and International Security, have declared that the use of information and communication technology (ICTs) by nations, should be governed by current international law (Hollis and Hollis, 2021). International law being the collection of rules governing relations between states (Shaw, 2016). Currently there is no international law specifically governing the global cyberspace realm, and it’s still being established how exactly international law applies to cyberspace as a whole.

Having established the need to define cyberspace in the context of international law and security, the United Nations (UN) elected 25 representatives from various countries. They named them, The Group of Governmental Experts (GGE) and in 2019 held their first meeting. In 2021 GGE released a report outlining certain international laws as a guideline for member States to follow. The top seven States submitting the most detailed and comprehensive positions on how international law applies in cyberspace (included in the annex of the GGE report) were; Australia, Estonia, France, Germany, Netherlands, United Kingdom, and United States. From these submissions, four distinct rules have been outlined, which may be applicable in the context of cyber operations. These are; “the obligation to respect the sovereignty of other States, the obligation not to intervene into the internal affairs of other States, the prohibition of the use of force and an obligation of due diligence” (Roguski, P. 2020).

The Netherlands references navigation of international law and cyberspace by using The Tallinn Manual 2.0, which is often referred to as ‘a guide to travel through cyberspace’. This manual focuses on cybercrime during peace time and the Netherlands has also made significant contributions to the development of the manual (Zandbergen, 2017).

**5.0 GDPR**

The General Data Protection Regulation (GDPR) applies to countries that do business in or with the EU. The law came into effect on 25 May 2018, in the Netherlands it is called Algemene Verordening Gegevensbescherming (AVG). The Dutch data protection authority (AP) is the supervisory authority for both guidance and enforcement of the privacy regulation. Unlike International Law, GDPR is specific to all independent entrepreneurs who process personal data (business.gov.nl, 2018). This provides the legal and ethical protection of personal identifiable information.

**6.0 Ethical Considerations**

Ethics is a philosophical science drawn from man’s consciousness of what is wright and wrong (Tuana, N., 2010). Ethical norms have translated into a countries customs and their laws of society. The Netherlands currently has no defined ethical laws in place within the cyberspace realm. However, the basic ethical considerations of data protection have been addressed with the inception of GDPR. Keeping data safe seemingly remains the primary cyber concern of most States considered above. Personal privacy, data access rights, and dangerous online behaviour are also fundamental ethical concerns pertaining the use of Information Technology (IT) on international networks. Such concerns can be addressed by implementing protective technologies such as Encryption, Digital IDs, SSL and Firewalls (Gunarto, 2020).

Interestingly, the worlds largest technical professional organization, the Institute for Electrical and Electronics Engineers (IEEE), has a sector entirely devoted to technology ethics. In areas such as artificial intelligence (AI), robotics and data management, the IEEE is working on new ethical standards (Vallor, William and Rewak, 2016). Once released this is likely to be a useful guide on ethical considerations within the realm of cyberspace.

A popular case of ethical consideration and one that sparked a lot of debate globally was that of Edward Snowden, who had allegedly stole and leaked classified files from the National Security Agency (NSA). He believed that the USA and the NSA were collecting too much personal information on the wrong people and that the NSA was violating, unjustifiably, the privacy of law-abiding Americans (Future of Tech, 2021).

**7.0 Conclusion**

Arguably the Netherlands is a country both technically forward thinking and innovative. A global leader in logistics and distribution, with a strong technical ecosystem and focus on digital infrastructure, technology, and transformation. It’s ranked second in the world for online connectivity and is home to Europe’s largest security cluster, The Hague Security Delta (HSD). The Cyber Security Assessment Netherlands 2021 (CSAN) outlined the threat of ransomware as a global problem and one that could potentially be a threat to national security. They have outlined a promising solution to the threat of ransomware that lies in increasing the costs to criminals who will have to weigh this against any benefits gained from an attack (Veiligheid, 2021).

The NCSC’s mission is to enhance the resilience of Dutch society and to form a strong, stable digital domain. The progress of this mission shows as the NCSC continually advances its cyber security framework every two years (Privacy Solved, 2022). The Dutch police having implemented their global “No more Ransom” campaign is another success marker which has helped millions of citizens and many companies (Nomoreransom.org, 2019). The Netherlands continues to support global initiatives, ethical views, European co-operation, and leans forward as a predominant example of an active and effective cybersecurity landscape.

**8.0 References**  
Startup and Places 2022, Release Startup Heatmap Europe 2022  
Accessible: https://startupsandplaces.com/release-startup-heatmap-europe-2022/ [Accessed 12 July 2022]

NFIA. 2022. IT & Tech. [online] Available at: <https://investinholland.com/doing-business-here/industries/it-tech/> [Accessed 12 July 2022].

Paganini, P. (2021). The Netherlands declares war on ransomware operations. [online] Security Affairs. Available at: https://securityaffairs.co/wordpress/123113/security/the-netherlands-war-ransomware-operations.html [Accessed 19 Jul. 2022].

Federal Bureau of Investigation (2021). Ransomware. [online] Federal Bureau of Investigation. Available at: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware. [Accessed 12 Jul. 2022].

The EE. (2020). Netherlands tops european countries at greatest risk of cyber-crime. [online] Available at: https://www.theee.ai/2020/02/24/1289-netherlands-tops-european-countries-at-greatest-risk-of-cyber-crime/ [Accessed 19 Jul. 2022].

NL Times. (2022). Cyber threat increasing faster than Dutch companies’ resilience. [online] Available at: https://nltimes.nl/2022/07/04/cyber-threat-increasing-faster-dutch-companies-resilience [Accessed 19 Jul. 2022].

Share 4PL. (2021). The Netherlands as your entry to European markets. [online] Available at: https://share4pl.com/the-netherlands-as-entry-to-european-markets/ [Accessed 19 Jul. 2022].

www.europarl.europa.eu. (2022). Cybersecurity: main and emerging threats in 2021 (infographic) | News | European Parliament. [online] Available at: https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats-in-2021-infographic#ssh [Accessed 11 Jul. 2022].

Shaw, M. (2016). International law. In: Encyclopædia Britannica. [online] Available at: https://www.britannica.com/topic/international-law.

Hollis, D. and Hollis, D. (2021). A Brief Primer on International Law and Cyberspace. [online] Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763.

Roguski, P. (2020), Application of International Law to Cyber Operations: A ComparativeAnalysis of States’ Views.The Hague Program For Cyber Norms Policy Brief.

Zandbergen, A. (2017). Tallinn Manual 2.0 guides governments through cyberspace» Embassy of the Netherlands. [online] Embassy of the Netherlands. Available at: https://nlintheusa.com/tallinn-manual-2-0-guides-governments-cyberspace/ [Accessed 21 Jul. 2022].

business.gov.nl. (2018). How to make your business GDPR compliant. [online] Available at: https://business.gov.nl/running-your-business/business-management/administration/how-to-make-your-business-gdpr-compliant/ [Accessed 19 Jul. 2022].

Vallor, S., William, J. and Rewak, S. (2016). An Introduction to Cybersecurity Ethics. [online] Available at: https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf.

Gunarto, H. (2020). Ethical Issues in Cyberspace and IT Society. [online] Available at: https://www.apu.ac.jp/~gunarto/it1.pdf.

Future of Tech (2021). Ethical Issues in Cybersecurity. [online] CompTIA’s Future of Tech. Available at: https://www.futureoftech.org/cybersecurity/4-ethical-issues-in-cybersecurity/.

Privacy Solved. (2022). Cybersecurity: Focus on the Netherlands’ Information Security Outlook – PrivacySolved. [online] Available at: https://www.privacysolved.com/cybersecurity-focus-on-the-netherlands-information-security-outlook/ [Accessed 22 Jul. 2022].

digital-strategy.ec.europa.eu. (2021). Broadband in the Netherlands | Shaping Europe’s digital future. [online] Available at: https://digital-strategy.ec.europa.eu/en/policies/broadband-netherlands.

Europol. (2021). No More Ransom: how 4 millions victims of ransomware have fought back against hackers. [online] Available at: https://www.europol.europa.eu/media-press/newsroom/news/no-more-ransom-how-4-millions-victims-of-ransomware-have-fought-back-against-hackers [Accessed 22 Jul. 2022].

Nomoreransom.org. (2019). The No More Ransom Project. [online] Available at: https://www.nomoreransom.org/en/index.html.

Tuana, N., 2010. Leading with ethics, aiming for policy: New opportunities for philosophy of science. Synthese, 177(3), pp.471-492.

Veiligheid, M. van J. en (2021). Cyber Security Assessment Netherlands 2021 - Publication - National Coordinator for Security and Counterterrorism. [online] english.nctv.nl. Available at: https://english.nctv.nl/documents/publications/2021/08/05/cyber-security-assessment-netherlands-2021 [Accessed 22 Jul. 2022].