**The dissemination of insights to parties that need those insights**

In the subsection above, we refer to different types of investigations into occurrences. The information generated by these investigations is only published in a limited number of cases: when, by way of exception, the organization opts to publish, or is required to do so by the regulator. In the previous subsection, we took as examples Maastricht University, the University of Amsterdam/University of Applied Sciences Amsterdam, the Municipality of Lochem and the Municipality Hof van Twente. We also suggested that the majority of investigations into occurrences are not published, or only within a closed circuit. The information is in fact only comprehensible for a limited group of experts, and that makes it appear an abstract, technical event. For that reason it is important when sharing insights from cyber-attacks to demystify them and to underline their human consequences.[215]

Moreover, at present there is no single entity that collects the information from investigations and reports for the purpose of scientific and/or statistical study. In the cyber domain, which enjoys a relatively new tradition in respect of incident investigation, there is a clear need for a platform where knowledge is shared and retained and where organizations can go in search of relevant insights to further improve their information security policy (historic capture). Incidentally, this aligns with the NCSC's mission as the National Cyber Security Center: to understand and interpret what is happening, to connect parties, knowledge and experience with the goal of preventing recurrence. [216]

In current practice, many organizations do not come clean about the fact that they have been attacked. The investigations do not provide the explanations needed to improve the system. Involved organizations do not share the lessons learned from occurrences outside their own organizations or communities.

## 4.5 Policy and the international context

At the European level, there are various regulations in the field of cybersecurity, as well as a number of initiatives under development. These regulations and initiatives each have a different purpose and target group. The table below lists some of the characteristics of the regulations.

215 Schaake, M., *The Lawless Realm, Countering the Real Cyberthreat.* 2020 https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm

216 https://www.ncsc.nl/over-ncsc, accessed on 13 September 2021.

| Legislative name | Type of legislation | Status | Content |
|---|---|---|---|
| NIS directive | Directive [217] | Should be implemented by Member States as of 10 May 2018.[218] | • Target audience: digital service providers and designated providers of essential services.<br>• Cooperation among member states on cybersecurity issues.<br>• Imposes obligations on target group to implement security requirements and report incidents. |
| NIS 2 directive | Directive | Draft directive. | • Target group: expanded from the NIS to include food sector, public administration, manufacturers of critical products, among others.<br>• More stringent security requirements for organizations and strengthening of European cooperation. |
| Cyber Security Act | Regulation[219] | In operation since 27 juni 2019. | • Target group: entire European digital market<br>• Expand the mandate of ENISA<br>• Introduce cybersecurity certification framework (still under development) |
| Digital Operational Resilience Act (DORA) | Regulation | Draft regulation, expected to enter info force end 2022. | • Target group: financial sector.<br>• Goal: harmonize rules on digital resilience in the EU.<br>• Basic framework for financial organizations, sets basic requirements for financial organizations including risk management and digital incidents. |
| Horizontal software regulation | Unknown | Under development. | • Target group: software manufacturers[220].<br>• Horizontal legislation regarding cybersecurity requirements for software products. |

In addition, there are also initiatives (in development) regulating Internet of Things (IoT), i.e. software that is part of other products. This includes the intention to set cybersecurity requirements for wireless devices via the Radio Equipment Directive and the regulation of connected devices in the Cybersecurity Resilience Act. In addition, a number of EU regulations were adopted in 2017 setting cybersecurity requirements for medical devices, and cybersecurity requirements will also be included in regulations for the automotive industry at UN level. Moreover, the general EU directive for product safety is being revised and will also include safety and security of products with digital components. There are also European developments in the field of consumer law for IoT products, which include, among others, matters relating to the right to updates.

217 A directive must be transposed into national law by the member states.
218 In the Netherlands, this is laid down in the Wbni.
219 A regulation is legislation directly applicable in all EU member states.
220 It is not yet clear for which specific target group this legislation is being developed.

Countering vulnerabilities in software, and investigating criminal acts for the purposes of enforcement and prosecution and the agreements on how States interact when it comes to cyberattacks all require international cooperation.[221]

The trade in software is an international market based on supply and demand. Manufacturers and end users are located throughout the world. As described in section 4.1, software as a product and the creation of that product throughout its lifecycle as a process are currently only regulated on the basis of legislation and regulations applicable to the domain in which the software is employed. For example software in vehicles and software in care institutions. Software itself is not subject to any government product or process regulations. There are however industry standards according to which a manufacturer can certify its software or processes, as a means of demonstrating accountability to its end users.

Actors who exploit vulnerabilities in software in order to attack the digital systems of organizations also come from all corners of the globe. They include criminal actors and actors working for nation states and combinations or hybrids of the two. Ransomware attacks, for example, are often carried out by criminal organizations, but often also serve as a cover for an operation by an intelligence service or as a way of generating income for a country. International cooperation is complex, partly because countries are not only the victims of unsafety through cyberattacks, but also benefit from vulnerabilities in software for their own activities.[222] In addition, ideological differences between countries are obstacles to international cooperation, for example disagreements on how States interact with the Internet and what actions against attackers (deterrence) are permissible.[223]

Nonetheless, the Member States of the European Union have shown over the past few years that they are able to enforce strict requirements on data protection and foreign investments, through cooperation. Countries also call each other to account (in public) more often after large-scale cyberattacks.

221 See also: Schaake, M., *The Lawless Realm, Countering the Real Cyberthreat*. 2020 https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm

222 Perlroth, N. *This is how they tell me the world ends: the cyberweapons arms race*, 2021.

223 Henriksen, A., The end of the road for the UN GGE process: The future regulation of cyberspace, *Journal of Cybersecurity*, Volume 5, Issue 1, 2019, tyy009, https://doi.org/10.1093/cybsec/tyy009. Fischerkeller, M.P. en R.J. Harknett, Deterrence is Not a Credible Strategy for Cyberspace. *Orbis*, Volume 61, Issue 3, 2017, Pages 381-393, 2017. Daniel, M., *Closing the Gap: Expanding Cyber Deterrence*. Cyberstability Paper Series, 2021.

Multistakeholder groups also make a contribution to improving international cooperation. The Global Commission on the Stability of Cyberspace has for example developed proposals for standards and policy that have improved international cybersecurity and stability. These are standards for responsible behaviour by both state and non-state actors, in cyberspace. This commission brings together a large number of stakeholders from different countries and from different types of organizations, such as governments, universities and manufacturers. They drew up eight standards, including the following:[224]

- Non-state actors may not carry out cyberattacks and states must prevent this and respond if it does happen.
- States must in principle report vulnerabilities of which they become aware to the manufacturer, and operate a transparent framework for when they decide not to do so.
- Manufacturers of products and services must give priority to cybersecurity and stability and do everything reasonably possible to ensure that they contain no vulnerabilities. They must also take measures to mitigate vulnerabilities of which they become aware, and be transparent about their actions. All actors have a duty to share information about vulnerabilities in order to prevent cyberattacks and to limit their consequences.
- Countries must take measures including legislation and regulations so that basic cyber hygiene is maintained.

224 GCSC, *Advancing Cyberstability*, 2019.https://cyberstability.org/report/