IEEE SA
STANDARDS ASSOCIATION

INDUSTRY CONNECTIONS REPORT

META ISSUES IN CYBERSECURITY

LAW AND CYBERSECURITY

Authored by

Samuli Haataja

EJ Wise

Louis de Koker

Pompeu Casanovas

RE Burnett

IEEE

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

PDF: STDVA27053 979-8-8557-0886-8

Find IEEE standards and standards-related product listings at: http://standards.ieee.org.

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA INDUSTRY CONNECTIONS DOCUMENTS

This IEEE Standards Association ("IEEE SA") Industry Connections publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the IEEE SA Industry Connections activity that produced this Work. IEEE and the IEEE SA Industry Connections activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE SA Industry Connections activity members disclaim any and all conditions relating to: results; and workmanlike effort. This IEEE SA Industry Connections document is supplied "AS IS" and "WITH ALL FAULTS."

Although the IEEE SA Industry Connections activity members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR IEEE SA INDUSTRY CONNECTIONS ACTIVITY MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at http://standards.ieee.org/about/sasb/iccom/.

This Work is published with the understanding that IEEE and the ICCom members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

TABLE OF CONTENTS

META ISSUES IN CYBERSECURITY: LAW AND CYBERSECURITY

ABSTRACT

As part of the IEEE Meta Issues in Cybersecurity project, this paper focuses on the legal aspects of cybersecurity. It provides an overview of the ways in which law creates rules, responsibilities, and obligations relevant to cybersecurity, and the limitations of the law in this context. While there is no standardized approach to regulating cybersecurity globally, Australia is used as an example to illustrate the patchwork of legal frameworks that have relevance to different aspects of cybersecurity. Law can be effective in imposing obligations on a range of stakeholders to help ensure effective cybersecurity measures and practices; however, there continue to be challenges in using law to advance cybersecurity. These include enforcing the law against those engaged in criminal activities that undermine cybersecurity, and the national security interests that nation-states can have in developing capabilities that undermine cybersecurity.

1. LEGAL ASPECTS OF CYBERSECURITY

1.1. BACKGROUND AND EXAMPLE OF AUSTRALIA

Various areas of law have relevance for different aspects of cybersecurity by creating rules for the conduct of different actors (such as individuals, corporations, and nation-states) in the cyber context. These areas of law include cybercrime provisions in criminal law; relevant cybersecurity-related obligations imposed on, for example, the operators of critical infrastructure; privacy protections under human rights law; directors' duties in corporate law; and public international law that provides a framework of established rules for the conduct of nation states their international cyber activities.

In Australia, for example, there is no single piece of law or legal framework around "cyber law." Instead, there are a patchwork of rights, obligations, and responsibilities that arise from various legal frameworks with relevance for different aspects of cybersecurity for different stakeholders. This patchwork of laws is illustrated by the "Cyber Law Mapping Project" that was conducted in 2021 in Australia.[1] The following sections summarize the topic categories and relevant legal frameworks outlined by this project.

1.1.1. COMMERCIAL ENTERPRISES

Commercial enterprises include the following:

- Contract law—Here cybersecurity threats can affect the drafting, performance, breach, and/or termination of contracts. Contract law can also be used to manage cyber risks and limit the liability of insurers and providers.
- Directors' duties—Here the law imposes a number of duties owed by the directors to the company and its shareholders. Engaging with cyber risks, and compliance with data breach notification laws are relevant in this context.[2]
- Mergers and acquisitions—Here the law regulates company takeovers. Cybersecurity is a part of this process, for example in relation to due diligence around cyber risk.

[1] "Australian Cyber Law Map" (Austlii, 2021) <https://austlii.community/wiki/CyberLaw/AustralianCyberLawMap>.

[2] Recent illustrations from the Australian Federal Court include, for example, ASIC v RI Advice where the Federal Court found Australian Financial Services licensee, RI Advice, breached its license obligations to act efficiently and fairly when it failed to have adequate risk management systems to manage its cybersecurity risks (Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496). Further, on continuous disclosure to shareholders – though not in relation to a cyber specific set of facts – the findings of ASIC v Getswift will be relevant for future litigation where cyber breaches are not disclosed (Australian Securities and Investments Commission v GetSwift Limited (Penalty Hearing) [2023] FCA 100). Efforts to claim legal professional privilege over cyber forensic and related materials were unsuccessful in Robertson v Optus where it was found that legal professional privilege applies to confidential communications made for the *dominant purpose* of the client obtaining legal advice or professional legal services in actual or anticipated litigation or regulatory investigations or proceedings (Robertson v Singtel Optus Pty Ltd [2023] FCA 1392).

1.1.2. CYBER OFFENCES

Cyber offenses include the following:

- Computer-based crime—Here the law provides criminal offenses around, for example, unauthorized access, denial-of-service attacks, phishing, and certain uses of malware. These laws are also relevant to "hacking back," that is, where someone seeks to hack a hacker's own network in response to a cybersecurity incident.

1.1.3. INFRASTRUCTURE

Infrastructure includes the following:

- Data—Here the law regulates public and private data (its use, storage, disposal, and so on).
- Healthcare—Here the law regulates healthcare information and records.
- Real property law—Here the law regulates land-related transactions (e.g., land transfer) through an electronic conveyancing process.
- Security of critical infrastructure—Here the law seeks to improve the Federal Government's ability to respond to national security risks (such as cybersecurity risks) affecting critical infrastructure. The law increases transparency around ownership of critical infrastructure and empowers the government to direct the owner/operator of critical infrastructure to perform actions that reduce national security risks.
- Telecommunications—Here the law regulates the operation of telecommunications providers (including Internet Service Providers), including security and notification obligations.

1.1.4. INTERNATIONAL LAW

International law provides a framework of rules for the cyber activities of states. States have agreed that much of existing international law applies in the cyber context, but the precise contours of how it applies are still being developed by states.

1.1.5. NATIONAL SECURITY

National security includes the following:

- Counter-terrorism—Here the law provides various offenses to criminal acts of terrorism and empowers intelligence and law enforcement agencies to counter this threat (whether or not terrorism involves a cyber dimension).

- Defence exports and trade—Here the law regulates the trade and export of defence-related technologies. The law implements international legal obligations into domestic law.
- Espionage, sabotage, and foreign interference—Here the law creates criminal offenses for espionage, sabotage, and foreign interference activities (whether or not they involve a cyber dimension).
- Foreign influence and election security—Here the law criminalizes foreign "interference" (in contrast to foreign "influence," which is not criminalized). The law also provides transparency measures to help ensure that the nature and extent of foreign actors' influence are clear to the public.
- Intelligence and surveillance—Here the law regulates the intelligence gathering and surveillance powers of intelligence and law enforcement agencies. It allows these agencies to engage in activities that may involve compromising cybersecurity and that would normally be contrary to relevant criminal law provisions.

1.1.6. PERSONAL RIGHTS

Personal rights include the following:

- Consumer rights—Here the law provides consumers with various rights, including access and control of their data.
- Online content and services—Here the law regulates online content and various online activities. For example, the Online Safety Act 2021 gives the eSafety Commissioner powers to protect Australians (adults and children) across most online platforms and forums where people can experience harm. From 16 December 2023, providers of Social Media Services, App Distribution Services, Internet Carriage Services, Hosting Services, and Equipment Services must comply with the requirements under the applicable industry code. The industry code for Search Engine Services came into effect on 12 March 2024.
- Privacy law—Here the law regulates the personal information handling practices of businesses and creates data breach notification requirements.
- Tort law—Here the law on negligence has the potential to provide protections to a person in certain circumstances where their personal information is compromised due to a cybersecurity incident.
- Unsolicited communications—Here the law regulates unsolicited marketing/messaging (spam).

1.2. DISCUSSION

Importantly, Section 1.1 only provides a surface-level account of the relevant legal frameworks in Australia.

Other countries will have differing legal frameworks and approaches to these issues and areas of law. This means that, while there may be some similarities in content or approaches in some areas of law (for example, in criminal law where states have modeled their laws around the Cybercrime Convention or intend to do so around the proposed new United Nations Convention on Cybercrime),[3] there is no standardized approach to the regulation of cybersecurity globally.

As a generalization, the most problematic conduct by different actors resulting in issues for cybersecurity (i.e., that involves undermining cybersecurity) is unlawful conduct. For example, globally distributed ransomware can affect the cybersecurity of various actors in different sectors of society from individuals to critical infrastructure operators and governments. Depending on who is responsible for the use of the ransomware, there are likely to be relevant laws that render the behavior in question unlawful (e.g., criminal law provisions in most countries). As such, the lack of law is often not the main problem; rather, the problem involves issues around anonymity regarding the identity and location of the actors responsible who are capable of engaging in these activities with relatively low risk compared to similar activities in the real world. On an international level, these concerns are exacerbated by nation-state activities (from espionage to state-sponsored criminal activities) that involve undermining cybersecurity in other states given existing uncertainties in how international law applies in this context (i.e., states have not yet reached agreement on how all aspects of international law apply in the cyber context),[4] and given the challenges around attributing cyber operations to states (both technically and legally).[5] It is interesting to note in this context that the Australian government announced cyber sanctions on 23 January 2024 on Aleksandr Ermakov, a Russian individual, for his role in the breach of the Medibank Private network in 2023, which led to the theft of 9.7 million records, some of which were then published on the dark web.[6] This is in line with the trend of states using various legal and diplomatic means to impose costs on those individuals responsible for cybersecurity incidents. The competing interpretations about how the law applies are also a site of political contestation among states with competing values, interests, and visions about the role of international law and institutions in a rules-based international order.

[3] See *Convention on Cybercrime*, opened for signature 23 November 2001, ETS No 185 (entered into force 1 July 2004); see also https://unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_sixth_session/main.

[4] For an overview of the official position of a number of states, see "Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266" UN Doc A/76/136* (13 July 2021).

[5] See Nicholas Tsagourias and Michael Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges" (2020) 31(1) *European Journal of International Law* 941.

[6] Joint media release Senator the Hon Penny Wong, the Hon Richard Marles MP, Deputy Prime Minister, Minister for Defence, the Hon Clare O'Neil MP, Minister for Home Affairs, Minister for Cyber Security, *Cyber sanctions in response to Medibank Private cyber attack* 23 January 2024 <https://www.foreignminister.gov.au/minister/penny-wong/media-release/cyber-sanctions-response-medibank-private-cyber-attack>

1.3. SCOPE AND CHALLENGES

The law can be effective in imposing obligations on a range of stakeholders to help ensure effective cybersecurity measures and practices, and law is an important avenue through which these stakeholders can be held accountable for poor cybersecurity. But there are also a range of challenges in using law to ensure cybersecurity because of the following:

- Lawbreakers will always exist. Even if there are laws in place prohibiting conduct, there are actors who will have an interest in engaging in unlawful conduct. The cyber context also makes this easier and less risky.
- Enforcement of the law can be challenging. Those whose conduct undermines cybersecurity can operate globally and given the nature of the Internet, these actors can obfuscate their geographical location, use proxies, and/or otherwise maintain a degree of anonymity and plausible deniability of their actions. This makes identification of those responsible, and enforcement of the law difficult. Imposing legal obligations to ensure cybersecurity for those stakeholders who can be held accountable (such as corporations and data subjects) through, for example, civil penalties, can be effective in limiting opportunities for cybersecurity breaches.
- Enforcement mechanisms may be lacking. For example, under international law there are few centralized enforcement mechanisms and states must generally adopt "self-help" measures in response to violations of the law.[7] Given the debate about how the law applies, it is not always clear when a cyber operation violates international law, and this has implications for the responses/recourse available to the victim state.[8]
- While the focus is often on criminals, whether individuals or as groups, as perpetrators, states also have a national interest in developing capabilities that undermine the cybersecurity of, for example, commercial software and foreign government entities. These capabilities may be used for a variety of purposes, for example for national commercial gain or political espionage purposes; for offensive cyber operations; for political propaganda purposes; for illegal evasion of international sanctions; etc. Some of these actions, such as offensive cyber operations, may involve violations of international law, but enforcement mechanisms may be lacking, and correct attribution may be complex. Other actions, such as political and commercial espionage, may not be illegal under international law but are generally criminalized by national laws.

[7] See Henning Lahmann, *Unilateral Remedies to Cyber Operations* (Cambridge University Press 2020).
[8] On how international law is considered to apply in this context, see, for example Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017).

1.4. RECOMMENDED AREAS FOR INVESTIGATION

The following areas are recommended for further investigation:

- Identify areas of the law that have been standardized through relevant model laws or international law.
- Identify aspects of relevant legal frameworks and cybersecurity governance that can be improved through standardization.
- Identify international best practices around relevant cybersecurity laws that could be used as a basis for standardization.

2. REFERENCES

The following sources have either been referenced within this paper or may be useful for additional reading:

[1] "Australian Cyber Law Map" (Austlii, 2021). <https://austlii.community/wiki/CyberLaw/AustralianCyberLawMap>.

[2] Australian Securities and Investments Commission v GetSwift Limited (Penalty Hearing) [2023] FCA 100.

[3] Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496.

[4] *Convention on Cybercrime*, opened for signature 23 November 2001, ETS No 185 (entered into force 1 July 2004).

[5] Joint media release Senator the Hon Penny Wong, the Hon Richard Marles MP, Deputy Prime Minister, Minister for Defence, the Hon Clare O'Neil MP, Minister for Home Affairs, Minister for Cyber Security, *Cyber sanctions in response to Medibank Private cyber attack* 23 January 2024. <https://www.foreignminister.gov.au/minister/penny-wong/media-release/cyber-sanctions-response-medibank-private-cyber-attack>.

[6] Henning Lahmann, *Unilateral Remedies to Cyber Operations* (Cambridge University Press 2020).

[7] Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017).

[8] Nicholas Tsagourias and Michael Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges" (2020) 31(1) *European Journal of International Law* 941.

[9] "Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266" UN Doc A/76/136* (13 July 2021).

[10] Robertson v Singtel Optus Pty Ltd [2023] FCA 1392.

RAISING THE WORLD'S STANDARDS

3 Park Avenue, New York, NY 10016-5997 USA http://standards.ieee.org

Tel.+1732-981-0060 Fax+1732-562-1571