INTERNATIONAL JOURNAL OF

Cyber Warfare and Terrorism

IGI PUBLISHING

Publisher of Peer-Reviewed, Timely, and Innovative Research Since 1988

www.igi-global.com

Table of Contents

International Journal of Cyber Warfare and Terrorism

Volume 10 • Issue 3 • July-September-2020 • ISSN: 1947-3435 • eISSN: 1947-3443

Special Issue of CWAR 2018

Editorial Preface

Research Articles

The *International Journal of Cyber Warfare and Terrorism* is indexed or listed in the following: Bacon's Media Directory; Cabell's Directories; DBLP; Google Scholar; INSPEC; MediaFinder; ProQuest Advanced Technologies & Aerospace Journals; ProQuest Computer Science Journals; ProQuest Illustrata: Technology; ProQuest Military Collection; ProQuest SciTech Journals; ProQuest Technology Journals; SCOPUS; The Index of Information Systems Journals; The Standard Periodical Directory; Ulrich's Periodicals Directory; Web of Science; Web of Science Emerging Sources Citation Index (ESCI)

International Journal of Cyber Warfare and Terrorism
Volume 10 • Issue 3 • July-September 2020

Cyber Warfare:
An Enquiry Into the Applicability of National Law to Cyberspace

Helaine Leggat, ICTLC Australia Pty Ltd, Melbourne, Australia

ABSTRACT

The Tallinn Manual on the International Law Applicable to Cyber Warfare (2013) sets out ninety-five 'black-letter rules' governing conflicts and the basis for each in treaty and customary law. An earlier version of this article considered the applicability of national law to cyberspace. Specifically, whether there was sufficient basis at a national law level to establish norms for acceptable behavior at an international level. The proposition being it is time for a new kind of international cooperation in relation to cyber warfare and acceptable norms of behavior in cyberspace. This article provides detail from various national statutes to illustrate how national law applies to cyberspace. Both papers consider the applicability of current national criminal and tort law by using hypothetical scenarios in relation to self-defence, conspiracy and corporate responsibility in the private sector. The intention is to encourage experts to cooperate internationally to recognise national rules equivalent to the Tallinn work.

KEYWORDS

Conspiracy, Corporate Responsibility, Cyber Security, Cyber Warfare, Cyberlaw, Cyberspace, International Law, National Law, Self-Defence, Tallinn Manual

1. INTRODUCTION AND BACKGROUND

1.1. Charter of the United Nations 1945

The Charter of the United Nations of 1945 (U.N. Charter) records the wish to save succeeding generations from war; respect treaty obligations and international law; and maintain international peace and security. Specifically, it records that armed force shall not be used, save in the common interest.

The purposes of the U.N. Charter, Article 1 include taking collective measures for the prevention and removal of threats to peace and acts of aggression. Principles for achieving the objectives include settling international disputes by peaceful means that maintain international peace, security and justice, and refrain from force against the territorial integrity or the political independence of any state. Significantly, Article 51 recognises the inherent right of individual or collective self-defence if an armed attack occurs.

DOI: 10.4018/IJCWT.2020070103

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of SELF-DEFENCE shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security (U.N. Charter Article 51).

The Charter of the United Nations, it's Additional Protocol 1 (1977), and the Geneva Conventions (1864 – 1949)[2] cater for pre-digital armed conflict.[3] A voluminous and well documented record of military and academic literature on the evolution to digital conflict exists, which includes, what is now recognised as 'cyberwar' and 'cyber warfare'. This paper, like the Tallinn Manual (2013) uses the terms 'cyberwar' and 'cyber warfare' in a purely descriptive, non-normative sense.

The regulatory framework relating to cyberwar and cyber warfare referenced in this enquiry is recorded in Additional Protocol 1 (1977), as (i) comprising international agreements (treaty law), (ii) the principles of international law derived from established custom, (iii) the principles of humanity, and (iv) the dictates of public conscience.

This background is included for context, and as a starting point for what I call the pre-digital system of legal order that has supported human societies for decades, and which has disintegrated as a result of the internet. It is this disintegration that propels the intended outcomes of this paper. Namely, to cooperate internationally by recognising national rules that already exist, and agreeing that these become new international norms for behaviour in cyberspace.

1.1.1. Precedent

At the outset, I would like to point to precedent in support of my contention that private enterprise, under national law, has been, and can continue to be, instrumental in shaping new international norms based on agreement through the law of contract. I believe this points to international solutions in relation to cyber warfare.

1.1.2. Lex Mercatoria

During the Middle Ages, merchants travelling across Europe to trade fairs, markets and seaports needed common ground rules to create trust and confidence for robust international trade. The differences amongst local feudal, royal and ecclesiastical law provided a significant degree of uncertainty and difficulty for the merchants operating in international markets (Reidenberg, 1998).

Custom and practice evolved into a distinct body of law known as *Lex Mercatoria,* a body of law independent of national laws which assured commercial participation and basic fairness in international trade relationships based on contract and consensus, despite the national law differences.

1.1.3. Lex Informatica

In the digital age participants travelling across information systems have confronted the same unstable and uncertain environments due to numerous national laws, changing rules and conflicting regulations which have arisen as a result of history, culture and religion, that are just as important for participants of the information society as the *Lex Mercatoria* was to merchants hundreds of years ago (Reidenberg, 1998).

Some twenty years ago, international consensus was reached by nations coming together to cooperate in the interests of international digital trade. The result was the recognition and facilitation of electronic transactions and communications as a result of the United Nations Commission of International Trade Law (UNCITRAL) model laws and conventions. To date, UNCITRAL has been responsible for the Model Law on Electronic Commerce, adopted in June 1996; the Model Law on Electronic Signatures, adopted in July 2011, and the Convention on the Use of Electronic

Communications adopted in November 2005 which have shaped the modernisation and harmonisation of electronic commerce. The connection with cyberwar is that it is the startling success of the digital economy and human nature (including greed, opportunism and power politics), that have led to the breakdown of old norms and the need to find consensus on how we might restore trust and certainty to international relationships.

1.1.4. Social Media, Terms and Conditions

Social media behemoths, as private sector entities, regulate the behaviour of their enormous communities through the law of contract in the form of terms and conditions of the use of their platforms. This is *Lex Mercatoria* and *Lex Informatica* in operation. Billions of civilians from innumerable jurisdictions consent to behave in an acceptable manner.

My contention is that private sector entities can similarly cooperate to establish norms of behaviour that would result in new and acceptable forms of behaviour in cyberspace.

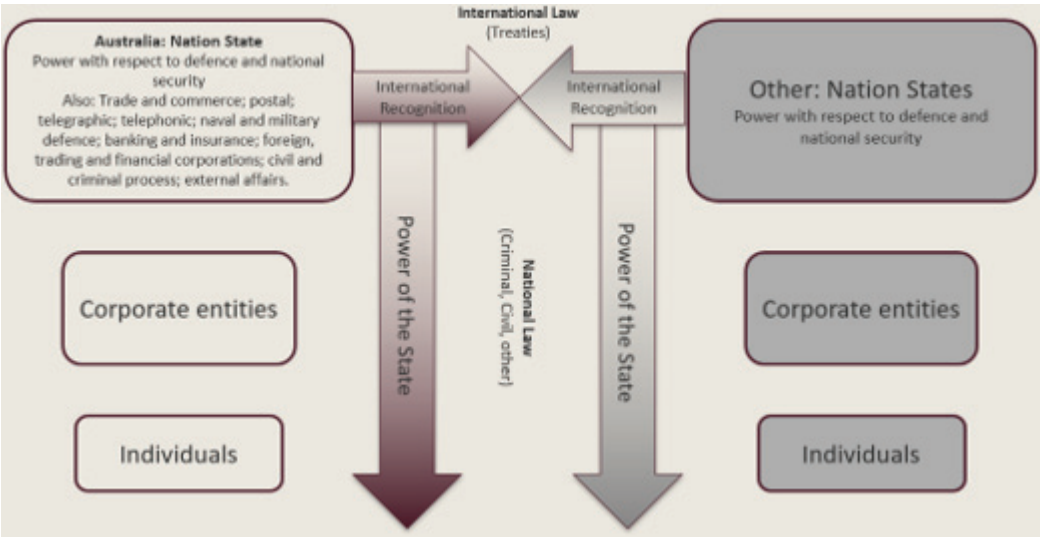
2. THE CHANGING FACE OF WARFARE (HYBRID AND ASYMMETRIC)

2.1. Traditional Wars

Traditional forms of warfare (land, sea, air, space) and early forms of digital warfare such as Stuxnet were confined to conflict between states as sovereign entities. Conflict, even armed conflict, between sovereign entities and their own corporate entities or civilians was not typically recognised as 'war.'

International law (public) governs the relationships between international sovereign states and entities as largely 'equal', being horizontal in power. National laws govern the relationships between sovereign states and their own corporate entities and civilians. Here, power is not equal. These are vertical relationships of power, where the state has power over its corporate entities and civilians (Figure 1).

Figure 1. Relationships of power

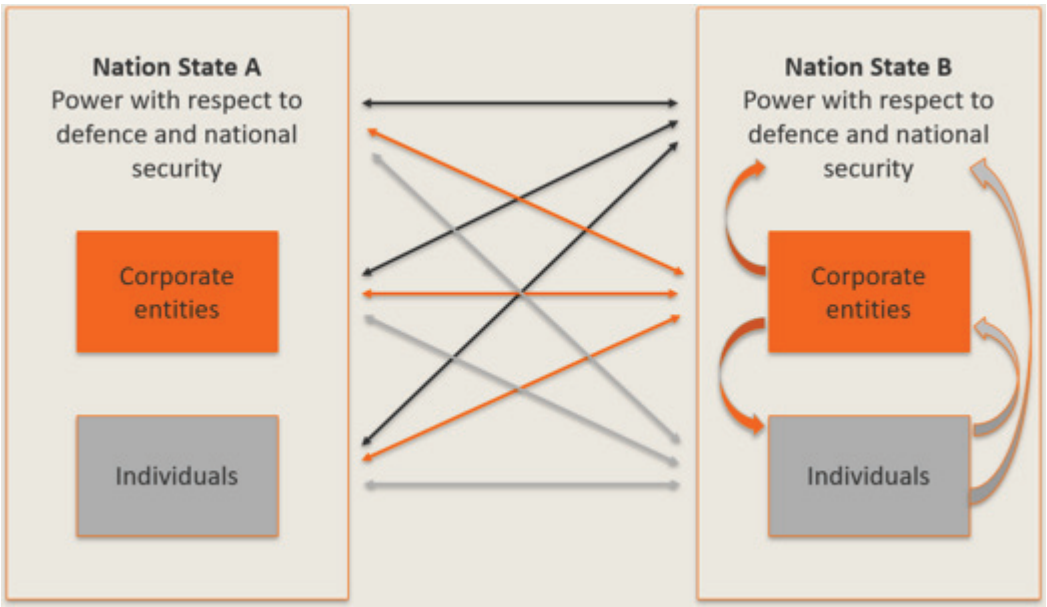


A breakdown in horizontal relationships in international law can lead to war, usually instigated at the behest of a government which is responsible for national security. A breakdown of vertical relationships in national law leads to law enforcement by the executive arm of the incumbent government.

The last decades have seen a breakdown of the system of global order, specifically in relation to the horizontal and vertical structures of power.

In my view, the breakdown in the vertical and horizontal structures of order, demands a new approach – enabling private sector organisations to better protect themselves through recognising rights (and obligations) in existing laws (Figure 2).

Figure 2. Structures of power



2.2. New Wars

From the time that sovereign states began to trade in, and stockpile zero day exploits as digital weapons; when sovereign states began to use cyberwar tactics (Zetter, 2014); when states sponsored proxies; when criminal organisations and individuals became guns for hire; when technology service providers 'partnered' with governments to weaken trust (Zetter, 2014); when foreign influence changed democracy; when IP theft was measured in billions of dollars; when threats to individual privacy became equal to national security, from then, traditional war, was 'new' war. Hybrid. Asymmetric.

The first paper on this topic records the different positions held between the Australian Federal Government and the Australian Department of Foreign Affairs and Trade. The former promulgating a raft of data-related laws; the latter on record for wanting no new laws, either model laws or conventions in relation to data (cyber). If we are to have no new laws, we need to work with the laws we have in order to address new war situations. The stability of global order based on the rule of law, learned from two great wars has dissipated.

One result is that:

Private sector entities operate today on the front lines of cyber conflict, targeted by a variety of hostile actors that seek to steal and misappropriate their intellectual property, degrade their infrastructure, and disrupt their business activities. Despite this reality, the options available within the private sector for responding to cyber threats are outdated and constrained. The status quo is reactive in nature and advantages the attacker. (Center for Cyber and Homeland Security George Washington University, 2016)

I believe that it is essential to empower private sector entities. I also believe it is imperative to do so in an ordered manner, under the rule of law and with respect to the law of different jurisdictions. This is why I advocate an approach that recognises similarities in different national legal systems, and effectively seeks to establish a common standard.

3. THE ENQUIRY

3.1. Approach

Like the earlier work, this enquiry into whether there is sufficient basis at a national law level to establish norms for acceptable behaviour at an international level has involved an examination of relevant aspects of:

1. *Tallinn Manual on the Law Application to Cyber Warfare* (2013);
2. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017);
3. Hypothetical Scenarios to Introduce Topics for Consideration in Relation to Criminal, Tort and Common Law, and Self-Defence, Conspiracy and Corporate Responsibility in the Private Sector;
4. National Laws of the Following Jurisdictions: Australia, New Zealand, USA, UK, China, Singapore and India.

The scope constraints in presenting the detailed research undertaken for the first paper, have to some extent been overcome in this paper by introducing sample excerpts from laws demonstrating the applicability of extending the Tallinn logic to private sector organisations through national laws.

4. CYBER ATTACK, FRAMEWORK AND SCENARIOS

4.1. Definition of a Cyber-Attack and Applicability

Tallinn (2013) defines a 'cyber-attack' as:

'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.'

The definition applies equally in international and non-international armed conflict (Rule 92. Tallinn 2.0). i.e. the principles of international law outlined in the Tallinn Work applies to the scenarios. The Tallinn Work is included as a frame of reference for the examination of national laws.

4.2. Scenario: Bank (Private Sector)

Current DDoS attack against online banking systems, exploiting client devices. Attacker seeks to obtain client credentials to commit theft. Bank knows location of the Command and Control (C&C) server of the attacker.

4.3. Issues Arising (Some Examples and Findings)

1. Timing is critical;
2. Timing is critical to lawfulness of the response (imminent, current, post attack);
3. Is a crime perpetrated against the bank, it's customers and/or third parties? (Yes);
4. Does tort law apply (wrongfulness in civil, as opposed to criminal law)? (Yes);
5. Does failure by the bank (its directors and officers) to act (or failure to act) constitute a failure in the exercise of due care and diligence, or negligence? (Yes);
6. Does the bank have a right or obligation to protect/defend the bank, its assets (money, property, infrastructure), it's customers or third parties (and their assets)? (Yes);
7. Does it matter who the attacker adversary is (organised crime, nation state attack, nation state proxy, individual, vigilante)? (No);
8. Does it matter who the attacker adversary is (organised crime, nation state attack, nation state proxy, individual, vigilante)? (No);
9. Does it matter who the attacker adversary is (organised crime, nation state attack, nation state proxy, individual, vigilante)? (No);
10. If so, does the right/obligation extend to self-defence? (Yes, but timing and other essentials determine liability, criminality etc.);
11. If so, does the right/obligation extend to pre-emptive action before the attack? (Yes. Comment above applies);
12. Does the bank have a right or obligation to gather intelligence (obtain evidence) on the C&C infrastructure of the attacker? (Yes);
13. If not, was an offence committed in obtaining intelligence? (Not necessarily. Manage contractually);
14. What if the bank attacks the C&C infrastructure of the attacker and this results in physical damage to property belonging to the perpetrators? (NA if principles of self-defence apply);
15. What if the bank attacks the C&C infrastructure of the attacker, and in the process takes down the revenue generating online businesses of innocent third parties compromised by the perpetrators in carrying out the attack against the bank? (Comment above applies. Manage risk contractually);
16. What if the bank attacks the C&C infrastructure of the attacker, and in the process causes personal injury or death to the attacker or innocent third party? (Principles of self-defence generally exclude death);
17. What if the bank attacks the critical infrastructure of the attacker, and in the process causes damage or destruction to the infrastructure of a foreign state? (This may constitute an act of war. *Mens rea* elements of a crime apply);
18. What if the bank contracts the services of an offshore organisation to provide defensive/offensive services, including employing targeted malware to cripple C&C infrastructure of an innocent third party? (Conspiracy and corporate responsibility for 'outsourcing' both have repercussions);
19. What if the bank employs the services of an offshore organisation to provide offensive services including deploying remote exploits to compromise the services/devices of the attacker (i.e. hack the hacker)? (Comment above applies);
20. Does the state have a duty or obligation to act? (Yes. However, it cannot possibly protect all of the private sector all of the time. It needs to recognise the applicability of existing law to cyberspace).

5. CONSOLIDATED ANALYSIS: TALLINN MANUAL AND TALLINN MANUAL 2.0 – RELEVANCE FOR NATIONAL LAWS AND CYBERSPACE

5.1. Approach to Analysis, Equivalence and Objective

The approach to the analysis and equivalence followed below employs a two-step process:

Step 1: Table 1 – Records the Rules in the Tallinn Manual, Tallinn Manual 2.0 and interpretation for private sector organisations; and
Step 2: Tables 2-12 - Record the application of samples of national laws.

The objective of the two-step analysis is to demonstrate that national laws apply to private sector organisations in cyberspace in just the same way the international law applies to cyberspace.

5.2. The Analysis – Step 1

See Table 1.

Table 1. Tallinn Manual (2013) and Tallinn Manual 2.0 (2017) – Relevance for National Laws and Cyberspace

Tallinn Manual on the Law Applicable to Cyber Warfare - 95 Black-Letter Rules.			Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations - 154 Black-Letter Rules	Interpretation for the Private Sector
Part I: International cyber security law.			Equivalent Rules.	Objective: Finding Equivalents for application in the Private Sector.
Section 1.	States and cyberspace. Sovereignty, Jurisdiction and Control.		Sovereignty. Note: Numbers in this column record the Rule numbers. And are not necessarily in chronological order.	Autonomy. Note: Interpreted under 6.1 as corporations law, self-defence and conspiracy.
	Rule 1 Sovereignty. *It is the sovereignty the state enjoys over territory that gives it the right to control cyber infrastructure and cyber activities within that territory.*	A state may exercise control over cyber infrastructure and activities within its sovereign territory.	1. The principle of state sovereignty applies in cyberspace.	The principle of organisational autonomy applies in cyberspace.
			2. The state enjoys authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations.	The organisation enjoys authority with regard to its corporate cyber infrastructure, persons, and cyber activities located within its premises, facilities and on its corporate networks (including where it has possession and control of data in other jurisdictions), subject to its national and international legal obligations.
			3. A state is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it.	An organisation is free to conduct cyber activities in its national and international business relations, subject to any contrary rule of national or international law binding on it.
			4. A state must not conduct cyber operations that violate the sovereignty of another state.	An organisation must not conduct cyber operations that violate the autonomy of another organisation.
			5. Any interference by a state with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty.	Any interference by an organisation with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of autonomy.

continued on following page

Table 1. Continued

Tallinn Manual on the Law Applicable to Cyber Warfare - 95 Black-Letter Rules.			Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations - 154 Black-Letter Rules	Interpretation for the Private Sector
NA.			Due Diligence.	
			6. A state must exercise due diligence in not allowing its territory, or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences, for other states.	A director must exercise due diligence in not allowing its organisation, or cyber infrastructure under its corporate control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences, for others.
			7. The principle of due diligence requires a state to take all measures that are feasible in the circumstances to put an end to cyber operations that affect the right of, and produce serious adverse consequences for, other states.	The principle of due diligence requires a director to take all measures that are feasible in the circumstances to put an end to cyber operations that affect the rights of, and produce serious adverse consequences, for others.
Section 2.	State responsibility.		International responsibility.	Organisational responsibility.
	Rule 6. Legal responsibility of states.	The state bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation. *Note: The causation of damage is not a precondition to the characterisation of the cyber operation as an internationally wrongful act under the law of state responsibility. Persons or entities specifically empowered by domestic law to exercise 'governmental authority' are equated to state organs. The state's involvement with non-state actors may itself constitute a violation of international law, even in cases where the actions of the non-state actors involved cannot be attributed to the state, for example a state that provides hacking tools that are subsequently employed by an insurgent group on its own initiative against another state. See also outsourcing (could be conspiracy) of hacking services.*	14. A state bears international responsibility for a cyber-related act that is attributable to the state and that constitutes a breach of an international legal obligation.	An organisation bears national and international responsibility for a cyber-related act that is attributable to the organisation and that constitutes a breach of a national or international legal obligation.
			15. Cyber operations conducted by organs of the state, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the state.	Cyber operations conducted by directors and officers of the organisation or by persons or entities empowered by domestic law to exercise elements of corporate authority, are attributable to the organisation (directors).
			16. Cyber operations conducted by an organ of a state that has been placed at the disposal of another state are attributable to the latter when the organ is acting in the exercise of elements of governmental authority of the state at the disposal of which it is placed.	Cyber operations conducted by directors and officers of the organisation that have been placed at the disposal of another organisation are attributable to the latter, when the organisation is acting in the exercise of elements of corporate authority of the organisation, at the disposal of which it is placed.

continued on following page

Table 1. Continued

Tallinn Manual on the Law Applicable to Cyber Warfare - 95 Black-Letter Rules.			Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations - 154 Black-Letter Rules	Interpretation for the Private Sector
			17. Cyber operations conducted by a non-state actor are attributable to a state when: – engaged in pursuant to its instructions or under its direction; or – the state acknowledges and adopts the operations as its own or under its control.	Cyber operations conducted by a non-organisational actor (third party) are attributable to the organisation when: – engaged in pursuant to its instructions or under its direction; or – the organisation acknowledges and adopts the operations as its own or under its control.
			18. With respect to cyber operations, a state is responsible for: – it's aid or assistance to another state in the commission of an internationally wrongful act and the state provides the aid or assistance knowing the circumstances of the internationally wrongful act and the act would be internationally wrongful if committed by it; – the internationally wrongful act of another state it directs and controls if the direction and control is done with knowledge of the circumstances of the internationally wrongful act and the act would be internationally wrongful if committed by it; (Ref – Outsourcing) or – an internationally wrongful act it coerces another state to commit.	With respect to cyber operations, an organisation is responsible for: – it's aid or assistance to another organisation in the commission of a wrongful act and the organisation provides the aid or assistance knowing of the circumstances of the nationally or internationally wrongful act and that the act would be wrongful if committed by it; – the wrongful act of another organisation it directs and controls if the direction and control is done with knowledge of the circumstances of the wrongful act and the act would be wrongful if committed by it; or – a wrongful act it coerces another organisation to commit.
			19. The wrongfulness of an act involving cyber operations is precluded in the case of: – Consent; – Self-defence; – Countermeasures; – Necessity; – Force majeure; or – Distress.	The wrongfulness of an act involving cyber operations is precluded in the case of: – Consent; – Self-defence; – Countermeasures; – Necessity; – Force majeure; or – Distress.
			20. A state may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another state.	An organisation may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of a national or international legal obligation that it is owed by another organisation.
			21. Countermeasures, whether cyber in nature or not, may only be taken to induce a responsible state to comply with the legal obligations that it owes an injured state.	Countermeasures, whether cyber in nature or not, may only be taken to induce a responsible organisation to comply with the legal obligations that it owes an injured organisation.
			22. Countermeasures, whether cyber in nature or not may not include actions that affect fundamental human rights, amount to prohibited belligerent reprisals, or violate a peremptory norm. A state taking countermeasures must fulfil its obligations with respect to diplomatic and consular inviolability.	Countermeasures, whether cyber in nature or not may not include actions that affect fundamental human rights, amount to prohibited belligerent reprisals, or violate a peremptory norm. An organisation taking countermeasures must fulfil its obligations with respect to national and international law.

continued on following page

Table 1. Continued

Tallinn Manual on the Law Applicable to Cyber Warfare - 95 Black-Letter Rules.			Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations - 154 Black-Letter Rules	Interpretation for the Private Sector
			23. Countermeasures, whether cyber in nature or not, must be proportionate to the injury to which they respond.	Countermeasures, whether cyber in nature or not, must be proportionate to the injury to which they respond.
			24. Only an injured state may engage in countermeasures, whether cyber in nature or not.	Only an injured organisation may engage in countermeasures, whether cyber in nature or not.
			25. A countermeasure, whether cyber in nature or not, that violates the legal obligation owed to a third state or other party is prohibited.	A countermeasure, whether cyber in nature or not, that violates the legal obligation owed to a third organisation or other party is prohibited.
			26. A state may act pursuant to the plea of necessity in response to acts that present a grave or imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding itself. (Necessity). (Ref: Take down the network).	An organisation may act pursuant to the plea of necessity in response to acts that present a grave or imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding itself. (Necessity).
			27. A responsible state must cease an internationally wrongful act committed by cyber means and, if appropriate, provide assurances and guarantees of non-repetition.	A responsible organisation must cease a nationally or an internationally wrongful act committed by cyber means and, if appropriate, provide assurances and guarantees of non-repetition.
			28. A responsible state must make full reparation for injury suffered by an injured state as the result of an internationally wrongful act committed by cyber means.	A responsible organisation must make full reparation for injury suffered by an injured organisation as the result of nationally or internationally wrongful act committed by cyber means.
			29. Reparations for injury suffered by an injured state as the result of an internationally wrongful act committed by cyber means may take the form of restitution, compensation, and satisfaction.	Reparations for injury suffered by an injured organisation as the result of a nationally or internationally wrongful act committed by cyber means may take the form of restitution, compensation, and satisfaction.
			30. Any state may invoke the responsibility of a state that has conducted cyber operations breaching and *erga omnes* obligation owed to the international community as a whole. (Owing to all).	Any organisation may invoke the responsibility of another organisation that has conducted cyber operations breaching and *erga omnes* obligation owed to the international community as a whole. (Owing to all).
			31. An international organisation bears international legal responsibility for a cyber operation that breaches and international legal obligation an is attributable to the organisation.	An organisation bears national and international legal responsibility for a cyber operation that breaches an international legal obligation and is attributable to the organisation.
	Rule 9. Countermeasures.	A state injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible state.		An organisation injured by a wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible organisation.

continued on following page

Table 1. Continued

Tallinn Manual on the Law Applicable to Cyber Warfare - 95 Black-Letter Rules.			Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations - 154 Black-Letter Rules	Interpretation for the Private Sector
	Rule 10. Prohibition of threat or use of force.	A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any state, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.	68. Prohibition of threat or use of force: A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any state, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.	Prohibition of threat or use of force: A cyber operation that constitutes a threat or use of force against the integrity (autonomy) or independence of any individual, organisation or state, or that is in any other manner inconsistent with the purposes of national or international law, is unlawful.
			69. A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of the use of force.	A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of the use of force.
			70. A cyber operation, or threat of cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be a lawful use of force.	A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force.
			71. Self-defence against armed attack: A state that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends upon its scale and effects.	Self-defence against armed attack: An organisation that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends upon its scale and effects.
			72. Necessity and proportionality: A use of force involving cyber operations undertaken by a state in the exercise of its right of self-defence must be necessary and proportionate.	Necessity and proportionality: A use of force involving cyber operations undertaken by an organisation in the exercise of its right of self-defence must be necessary and proportionate.
			73. Eminence and immediacy: The right to use force in self-defence arises if the cyber armed attack occurs or is imminent. It is further subject to requirement of immediacy.	Eminence and immediacy: The right to use force in self-defence arises if the cyber armed attack occurs or is imminent. It is further subject to the requirement of immediacy.
			74. Collective self-defence: The right of self-defence may be exercised collectively. Collective self-defence against a cyber operation amounting to an armed attack may only be exercised at the request of the victim state and within the scope of the request.	Collective self-defence: The right of self-defence may be exercised collectively. Collective self-defence against a cyber operation amounting to an armed attack may only be exercised at the request of the victim organisation and within the scope of the request.
			75. Measures involving cyber operations undertaken by states in the exercise of the right of self-defence Pursuant to Article 51 of the United Nations Charter shall be immediately reported to the United Nations Security Council.	Measures involving cyber operations undertaken by organisations in the exercise of the right of self-defence under national and international law shall be immediately reported to national authorities.

5.3. The Analysis – Step 2

Table 2 records detailed excerpts from the laws of Australia, China and Singapore on self-defence, conspiracy and corporate responsibility. These support the interpretation of the Tallinn Manual and the Tallinn Manual 2.0 as equivalent to the private sector. Tables 2-12 are the application of the samples of national laws applicable to the scenario.

5.3.1. Australia: Self - Defence

See Tables 2 and 3.

Table 2. Criminal Code Act 1995 (Cth)

		"property " includes: (a) real property; and (b) personal property; and (c) money; and (d) a thing in action or other intangible property; and (e) electricity.
10.4 Self-defence.	(1)	A person is not criminally responsible for an offence if he or she carries out the conduct constituting the offence in self-defence.
	(2)	A person carries out conduct in self-defence if and only if he or she believes the conduct is necessary: (a) to defend himself or herself or another person; or (b) to prevent or terminate the unlawful imprisonment of himself or herself or another person; or (c) to protect property from unlawful appropriation, destruction, damage or interference; or (d) to prevent criminal trespass to any land or premises; or (e) to remove from any land or premises a person who is committing criminal trespass; and the conduct is a reasonable response in the circumstances as he or she perceives them.
	(3)	This section does not apply if the person uses force that involves the intentional infliction of death or really serious injury: (a) to protect property; or (b) to prevent criminal trespass; or (c) to remove a person who is committing criminal trespass.
		This section does not apply if: (a) the person is responding to lawful conduct; and (b) he or she knew that the conduct was lawful. However, conduct is not lawful merely because the person carrying it out is not criminally responsible for it.

Table 3. Self-defence: Crimes Act 1958 (Vic)

SECT 322K.	Self-defence.	(1)	A person is not guilty of an offence if the person carries out the conduct constituting the offence in self-defence.
		(2)	A person carries out conduct in self-defence if— (a) the person believes that the conduct is necessary in self-defence; and (b) the conduct is a reasonable response in the circumstances as the person perceives them.
		(3)	This section only applies in the case of murder if the person believes that the conduct is necessary to defend the person or another person from the infliction of death or really serious injury.
SECT 322L.	Self-defence does not apply to a response to lawful conduct.		Section 322K does not apply if - (a) the person is responding to lawful conduct; and (b) at the time of the person's response, the person knows that the conduct is lawful.

5.3.2. Australia: Conspiracy

See Table 4.

5.3.3. Australia: Corporate Responsibility

See Table 5.

Table 4. Criminal Code Act 1995 (Cth)

11.5 Conspiracy.	(1)	A person who conspires with another person to commit an offence punishable by imprisonment for more than 12 months, or by a fine of 200 penalty units or more, is guilty of the offence of conspiracy to commit that offence and is punishable as if the offence to which the conspiracy relates had been committed.
	(2)	For the person to be guilty: (a) the person must have entered into an agreement with one or more other persons; and (b) the person and at least one other party to the agreement must have intended that an offence would be committed pursuant to the agreement; and (c) the person or at least one other party to the agreement must have committed an overt act pursuant to the agreement.

Table 5. Corporations Act 2001 (Cth)

Chapter 2D—Officers and employees Part 2D.1—Duties and powers.	SECT 179 Background to duties of directors, other officers and employees.	(1)	This Part sets out some of the most significant duties of directors, secretaries, other officers and employees of corporations. Other duties are imposed by other provisions of this Act and other laws (including the general law). (2) Section 9 defines both director and officer. Officer includes, as well as directors and secretaries, some other people who manage the corporation or its property (such as receivers and liquidators).
	SECT 180 Care and diligence—directors and other officers.	(1)	A director or other officer of a corporation must exercise their powers and discharge their duties with the degree of care and diligence that a reasonable person would exercise if they: (a) were a director or officer of a corporation in the corporation's circumstances; and (b) occupied the office held by, and had the same responsibilities within the corporation as, the director or officer.
	Business judgment rule.	(2)	A director or other officer of a corporation who makes a business judgment is taken to meet the requirements of subsection (1), and their equivalent duties at common law and in equity, in respect of the judgment if they: (a) make the judgment in good faith for a proper purpose; and (b) do not have a material personal interest in the subject matter of the judgment; and (c) inform themselves about the subject matter of the judgment to the extent they reasonably believe to be appropriate; and (d) rationally believe that the judgment is in the best interests of the corporation. The director's or officer's belief that the judgment is in the best interests of the corporation is a rational one unless the belief is one that no reasonable person in their position would hold.
		(3)	In this section: business judgment means any decision to take or not take action in respect of a matter relevant to the business operations of the corporation

5.3.4. China: Self-Defence

See Tables 6 and 7.

Table 6. Tort Law of the People's Republic of China 2009 (China)

Chapter III Circumstances to Waive Liability and Mitigate Liability.	Article 30.	Where any harm is caused by self-defence, the person exercising self-defence shall not be liable. If the self-defence exceeds the necessary limit, causing any undue harm, the person exercising self-defence shall assume proper liability.

Table 7. Criminal Law of the People's Republic of China 1997 (China)

Chapter II.	Section 1 Crimes and Criminal Responsibility.	Article 13	A crime refers to an act that endangers the sovereignty and territorial integrity and security of the state; dismembers the state and subverts the political power of the people's dictatorship and overthrows the socialist system; disrupts social order and economic order; violates property owned by the state or collectively owned by the working people; violates the citizens' privately owned property or infringes upon the citizens' rights of the person and their democratic and other rights; and any other act that endangers society and is punishable according to law. However, an act that is clearly of minor importance and little harm shall not be considered a crime.
		Article 20	Where a person conducts an act to stop an unlawful infringement in order to avert an immediate and unlawful infringement of the state's interest or of the public interest or of his own or another person's rights of the person, or property rights, or other rights, resulting in harm to the unlawful infringer, such an act shall be justifiable defence, and criminal responsibility shall not be borne for such an act. Criminal responsibility shall be borne if justifiable defence apparently exceeds the limits of necessity and causes serious harm; however, a mitigated punishment or exemption from punishment shall be given. Where a defence is conducted to an immediate violent crime of committing physical assault, committing homicide, robbery, rape, kidnapping, and other crimes seriously endangering the security of a person, and it causes bodily injury or death to the unlawful infringer, such an act shall not be defence that exceeds the limits of necessity, and criminal responsibility shall not be borne for such an act.
		Article 21.	Criminal responsibility shall not be borne for an act that a person is compelled to commit in an emergency to avert an immediate danger to the state's interest or the public interest or to his own or another person's rights of the person or property rights or other rights, and that causes harm. Criminal responsibility shall be borne if an act committed in an emergency to avert danger exceeds the limits of necessity and causes undue harm; However, a mitigated punishment or exemption from punishment shall be given. The provisions of the first paragraph of this Article with respect to averting danger to oneself shall not apply to a person who is charged with specific responsibility in his post or profession.

5.3.5. China: Conspiracy

See Table 8.

5.3.6. China: Corporate Responsibility

See Table 9.

Table 8. Criminal Law of the People's Republic of China 1997 (China)

Section 4 Crimes Committed by a Unit.	Article 30.	A company, enterprise, institution, organ, or public organisation that conducts an act harmful to society, where such an act is stipulated as a crime, shall bear criminal responsibility.
Section 1 Crimes of Disturbing the Public Order.	Article 285.	Whoever, in violation of state's stipulations, invades a computer information system involving the fields of state affairs, national defence construction or most advanced science and technology shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention.
	Article 286.	Whoever, in violation of state's stipulations, deletes, amends, adds or disturbs functions of a computer information system and causes the computer information system's inability to work normally shall, if serious consequences exist, be sentenced to fixed-term imprisonment of not more than five years or criminal detention. If especially serious consequences exist, the offender shall be sentenced to fixed-term imprisonment of not less than five years. Whoever, in violation of state's stipulations, conducts operations of deletion, amendment or addition towards data or application programmes which are stored, disposed of or transmitted in a computer information system shall, if serious consequences exist, be punished according to the provisions of the preceding paragraph. Whoever intentionally makes or disseminates computer virus or other destructive programmes and affects the normal operation of a computer information system shall, if serious consequences exist, be punished according to the provisions of the first paragraph.
Section 2 Crimes of Impairing Judicial Activities.	Article 310.	Whoever, while clearly knowing that another person has committed a crime, provides a concealed place or property for him, assists him in fleeing or provides false evidence to protect him shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention or public surveillance; if the circumstances are serious, the offender shall be sentenced to fixed-term imprisonment of not less than three years and not more than ten years. Conspirators to a crime mentioned in the preceding paragraph shall be punished as for a joint crime.

Table 9. Companies Law of the People's Republic of China 2005 (China)

Chapter I General Provisions.	Article 5.	In its operational activities, a company shall abide by laws and administrative regulations, observe social morals and commercial ethics, persist in honesty and good faith, accept supervision by the government and the public, and assume social responsibility.

5.3.7. Singapore: Self-Defence

See Table 10.

5.3.8. Singapore: Conspiracy

See Table 11.

Table 10. Penal Code 1872 (Singapore)

Chapter IV - General Exceptions.	Right of private defence.	96. Nothing is an offence which is done in the exercise of the right of private defence.
	Right of private defence of the body and of property.	97. Every person has a right, subject to the restrictions contained in section 99, to defend: (a) his own body, and the body of any other person, against any offence affecting the human body; (b) the property, whether movable or immovable, of himself or of any other person, against any act which is an offence falling under the definition of theft, robbery, mischief or criminal trespass, or which is an attempt to commit theft, robbery, mischief or criminal trespass.
	Acts against which there is no right of private defence.	99.(3) There is no right of private defence in cases in which there is time to have recourse to the protection of the public authorities.
	Extent to which the right may be exercised	(4) The right of private defence in no case extends to the inflicting of more harm than it is necessary to inflict for the purpose of defence.
	When such right extends to causing any harm other than death.	101. If the offence is not of any of the descriptions enumerated in section 100 (largely WRT threats of death and severe physical attacks) the right of private defence of the body does not extend to the voluntary causing of death to the assailant, but does extend, under the restrictions mentioned in section 99, to the voluntary causing to the assailant of any harm other than death.
	Commencement and continuance of the right of private defence of the body.	102. The right of private defence of the body commences as soon as a reasonable apprehension of danger to the body arises from an attempt or a threat to commit the offence, though the offence may not have been committed; and it continues as long as such apprehension of danger to the body continues.
	When the right of private defence of property extends to causing death.	103. The right of private defence of property extends, under the restrictions mentioned in section 99, to the voluntary causing of death or of any other harm to the wrongdoer, if the offence, the committing of which, or the attempting to commit which, occasions the exercise of the right, is an offence of any of the following descriptions: (a) robbery; (b) house-breaking by night; (c) mischief by fire committed on any building, tent or vessel, which building, tent or vessel is used as a human dwelling, or as a place for the custody of property; (d) theft, mischief or house-trespass, under such circumstances as may reasonably cause apprehension that death or grievous hurt will be the consequence, if such right of private defence is not exercised.
	When such right extends to causing any harm other than death.	104. If the offence, the committing of which, or the attempting to commit which, occasions the exercise of the right of private defence, is theft, mischief, or criminal trespass, not of any of the descriptions enumerated in section 103, that right does not extend to the voluntary causing of death, but does extend, subject to the restrictions mentioned in section 99, to the voluntary causing to the wrongdoer of any harm other than death.
	Commencement and continuance of the right of private defence of property.	105. - (1) The right of private defence of property commences when a reasonable apprehension of danger to the property commences. (2) The right of private defence of property against theft continues till the offender has affected his retreat with the property, or till the assistance of the public authorities is obtained, or till the property has been recovered. (3) The right of private defence of property against robbery continues as long as the offender causes or attempts to cause to any person death or hurt or wrongful restraint, or as long as the fear of instant death or of instant hurt or of instant personal restraint continues. (4) The right of private defence of property against criminal trespass or mischief, continues as long as the offender continues in the commission of criminal trespass or mischief. (5) The right of private defence of property against house-breaking by night continues as long as house-trespass which has been begun by such house-breaking continues.

Table 11. Penal Code 1872 (Singapore)

Each of several persons liable for an act done by all, in like manner as if done by him alone.	34. When a criminal act is done by several persons, in furtherance of the common intention of all, each of such persons is liable for that act in the same manner as if the act were done by him alone.
When such an act is criminal by reason of its being done with a criminal knowledge or intention.	35. Whenever an act, which is criminal only by reason of its being done with a criminal knowledge or intention, is done by several persons, each of such persons who joins in the act with such knowledge or intention, is liable for the act in the same manner as if the act were done by him alone with that knowledge or intention.
Co-operation by doing one of several acts constituting an offence.	37. When an offence is committed by means of several acts, whoever intentionally co-operates in the commission of that offence by doing any one of those acts, either singly or jointly with any other person, commits that offence.

5.3.9. Singapore: Corporate Responsibility

See Table 12.

6. CONCLUSION

6.1. In Summary

The objective of the two-step analysis is to demonstrate that national laws apply to private sector organisations in cyberspace in just the same way the international law applies to cyberspace.

Table 12. Companies Act 1967 (Singapore)

Part V. Management and Administration.	As to the duty and liability of officers.	157 (1)	A director shall at all times act honestly and use reasonable diligence in the discharge of the duties of his office.
	Powers of directors.	157A (1)	The business of a company shall be managed by, or under the direction or supervision of, the directors.
		(2)	The directors may exercise all the powers of a company except any power that this Act or the constitution of the company requires the company to exercise in general meeting.
			Subsection (1) shall apply to a director only if the director – (a) acts in good faith; (b) makes proper inquiry where the need for inquiry is indicated by the circumstances; and (c) has no knowledge that such reliance is unwarranted.

6.2. Findings

While only one scenario is included in this second paper. The issues arising and the answers as to what constitutes a legal response in almost any scenario is, I believe, clear from the kind of analysis summarised in 6 above.

My detailed research included laws of NZ, UK, US, Canada and India. All demonstrated substantially similar applicability.

6.3. Precedent and Risk

While it may take time for courts to provide legal certainty, it is my contention that the principles in the legal logic of the Tallinn work extend to apply to the private sector. Furthermore, I believe, that private sector organisations which do not consider these principles and apply them in assessing risk, fall short of their duties of diligence and care.

6.4. Final Comments – Paper 1 and 2

I have worked with international law in the field of cyberwar for well over a decade. I am fascinated at the general resistance of leaders, and I cite specifically those in policy and law, to consider the wealth of human history and knowledge that exists in legal systems across the world.

People are fundamentally the same. Our instinct for survival is primal – be it as individual civilians, as corporate citizens or as nation states.

I believe that at this critical time in the history of the world, we need to draw upon the wealth of our survival tactics, by resorting to the law and behaviours that are proven to have worked and agree to adapt and apply them to cyberspace and cyberwar scenarios and to 4IR societies.

Collectively, the private sector, with the cooperation of governments is positioned to raise the bar against malicious actors and to establish norms for acceptable behaviour in cyberspace.

We just need to agree to do so – as the merchants did all those years ago.

REFERENCES

Center for Cyber and Homeland Security. (2016). *Into the Gray Zone*. George Washington University. Retrieved from http://cchs.auburn.edu/_files/into-the-gray-zone.pdf

Companies Act 1967 (Singapore).

Companies Law of the People's Republic of China (2005). Retrieved from http://www.asianlii.org/cn/legis/cen/laws/cl119/

Corporations Act 2001 (2001).

Crimes Act 1958 (1958).

Criminal Code Act 1995 (1995).

Criminal Law of the People's Republic of China 1997 (China). (1997). Retrieved from http://www.asianlii.org/cn/legis/cen/laws/cl104/#2

International Committee of the Red Cross (ICRC). (1949, August 12). Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention). Retrieved from https://www.refworld.org/docid/3ae6b3694.html

International Committee of the Red Cross (ICRC). (1949, August 12). Protocol Additional to the Geneva Conventions and relating to the Protection of Victims of International Armed Conflicts (Protocol I). Retrieved from https://www.refworld.org/docid/3ae6b36b4.html

International Committee of the Red Cross (ICRC). (1949, August 12). Protocol Additional to the Geneva Conventions and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II).

Leggat, H. (2018, October). Cyber Warfare: An Enquiry into the Applicability of National Law to Cyberspace. *Paper presented at the 17th Australian Cyber Warfare Conference (CWAR)*. Academic Press.

Penal Code 1872 (Singapore).

Reidenberg, J. R. (1998). Lex Informatica: The formulation of Information Policy Rules Through Technology. *Texas Law Review*, *76*(3), 553–593. Retrieved from https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1041&context=faculty_scholarship

Schmitt, M. N. (Ed.). (2013). *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, United Kingdom: Cambridge University Press. doi:10.1017/CBO9781139169288

Schmitt, M. N., & Vihul, L. (Eds.). (2017). *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, United Kingdom: Cambridge University Press. doi:10.1017/9781316822524

Tort Law of the People's Republic of China 2009 (China). Retrieved from: http://english.www.gov.cn/archive/laws_regulations/2014/08/23/content_281474983043584.htm

UNCITRAL Model Law on Electronic Commerce (1996) with Additional Article 5 Bis as Adopted in 1998 Commission On International Trade Law. (1996). United Nations. Retrieved from uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

UNCITRAL Model Law on Electronic Signatures (2001) Commission On International Trade Law. (2001). United Nations. Retrieved from uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures

United Nations. (1945, October 24). Charter of the United Nations. Retrieved from https://www.refworld.org/docid/3ae6b3930.html

United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005) Commission On International Trade Law. (2005). United Nations. Retrieved from uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, NY: Crown Publishing Group.

ENDNOTES

[1] The Tallinn Manual examines the international law governing cyber warfare, with cyber warfare used in a purely descriptive, non-normative sense. Except when explicitly noted otherwise, the rules and commentaries in chapter 1 of the manual apply both in times of peace and in times of armed conflict (whether international or non-international in nature). During an international armed conflict, the law of neutrality also governs the rights and obligations of states in regard to cyber infrastructure and operations.

[2] The High Contracting Parties undertake to respect and to ensure respect for this Protocol in all circumstances. 2. In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.

[3] International humanitarian law distinguishes two types of armed conflicts, namely: international armed conflicts, opposing two or more States, and non-international armed conflicts, between governmental forces and non-governmental armed groups, or between such groups only. IHL treaty law also establishes a distinction between non-international armed conflicts in the meaning of common Article 3 of the Geneva Conventions of 1949 and non-international armed conflicts falling within the definition provided in Article 1 of Additional Protocol II.

IGI Global
DISSEMINATOR OF KNOWLEDGE
www.igi-global.com

Publisher of Peer-Reviewed, Timely, and
Innovative Academic Research Since 1988

IGI Global's Transformative Open Access (OA) Model:
How to Turn Your University Library's Database Acquisitions Into a Source of OA Funding

In response to the OA movement and well in advance of Plan S, IGI Global, early last year, unveiled their OA Fee Waiver (Offset Model) Initiative.

Under this initiative, librarians who invest in IGI Global's InfoSci-Books (5,300+ reference books) and/or InfoSci-Journals (185+ scholarly journals) databases will be able to subsidize their patron's OA article processing charges (APC) when their work is submitted and accepted (after the peer review process) into an IGI Global journal.*

How Does it Work?

1. When a library subscribes or perpetually purchases IGI Global's InfoSci-Databases including InfoSci-Books (5,300+ e-books), InfoSci-Journals (185+ e-journals), and/or their discipline/subject-focused subsets, IGI Global will match the library's investment with a fund of equal value to go toward subsidizing the OA article processing charges (APCs) for their patrons.

   Researchers: Be sure to recommend the InfoSci-Books and InfoSci-Journals to take advantage of this initiative.
2. When a student, faculty, or staff member submits a paper and it is accepted (following the peer review) into one of IGI Global's 185+ scholarly journals, the author will have the option to have their paper published under a traditional publishing model or as OA.
3. When the author chooses to have their paper published under OA, IGI Global will notify them of the OA Fee Waiver (Offset Model) Initiative. If the author decides they would like to take advantage of this initiative, IGI Global will deduct the US$ 1,500 APC from the created fund.
4. This fund will be offered on an annual basis and will renew as the subscription is renewed for each year thereafter. IGI Global will manage the fund and award the APC waivers unless the librarian has a preference as to how the funds should be managed.

Hear From the Experts on This Initiative:

"I'm very happy to have been able to make one of my recent research contributions, 'Visualizing the Social Media Conversations of a National Information Technology Professional Association' featured in the *International Journal of Human Capital and Information Technology Professionals*, freely available along with having access to the valuable resources found within IGI Global's InfoSci-Journals database."

– **Prof. Stuart Palmer**,
Deakin University, Australia

For More Information, Visit: www.igi-global.com/publish/contributor-resources/open-access or contact IGI Global's Database Team at eresources@igi-global.com.