State Cybersecurity Governance in the Fourth Industrial Revolution: An International Law Perspective

Jentley Lenong

Abstract The state remains the primary role player, which will determine cybersecurity policy and governance for the 4IR. The purpose of this chapter is to determine how states under international law should govern cybersecurity globally when faced with the disruptions that the 4IR will bring. The chapter uses the perceived future 4IR disruptions, prominent international law policy documents and the diversity of state practice to discern the prevailing normative order of state cybersecurity governance. The chapter identifies cyber justice as the desired foundational normative prescript to manage state cybersecurity governance and policy interventions. It further identifies two critical disruptions for state cybersecurity governance under a 4IR paradigm. These are the redundancy of customary legislative and regulatory intervention to legal and policy challenges and the threat to the notion of the state and state sovereignty through an evolved interpretation of cyber sovereignty as uncoupled from state territorial integrity. The research in the chapter is prescriptive. It provides a novel contribution for normative modelling of state cybersecurity governance under international law.

Keywords International law · Fourth industrial revolution (4IR) · State cybersecurity governance · Cyber justice · Cyber sovereignty · Normative governance

1 Introduction

At around 12:30 p.m. on 12 May 2017, computers of about ten hospitals across the United Kingdom were suddenly frozen and local files remotely encrypted by

J. Lenong (✉)
Department of Mercantile Law, University of Johannesburg, Corner University and Kingsway Road, Aucklandpark, Johannesburg, South Africa
e-mail: jentleyl@uj.ac.za

W. Doorsamy et al. (eds.), *The Disruptive Fourth Industrial Revolution*, Lecture Notes in Electrical Engineering 674,
https://doi.org/10.1007/978-3-030-48230-5_4

malware. Bewildered hospital staff were confronted with the malignant demand—pay $300 in Bitcoin in order to undo the cyber-attack.[1] The malware responsible for this cyber-attack was named "WannaCrypt/Wannacry" (Steyn 2017). WannaCry has been without a doubt the most widespread and devastating cyber-attack the world has up to date collectively experienced. It is estimated that between 400,000 and 1 million computers were affected by the malware (Venktess 2017). A global conference of skills pulled together and eventually, a patch for its vulnerability was released by Microsoft on the 14th of March 2017 (Pascariu et al. 2017), but not after the malware spread havoc across more than 150 countries. None of the more than 150 states affected by Wannacry had a rapid, decisive or concerted response to this cyber-attack.

This begs the question, who is burdened with the responsibility when it relates to transboundary emanating cyber-attacks? Under international law, the state remains primarily responsible for its citizens when faced with transboundary threats (Iyi 2016). Consequently, state cybersecurity governance[2] needs to be a central mechanism through which national cybersecurity policies and laws become operational. However, internationally state cybersecurity governance was particularly exposed by the Wannacry cyber-attack, with justice for the victims of these cyber-attacks - some of whom potentially could have lost their lives, still not having been achieved.

Under this reality, will the Fourth Industrial Revolution (4IR) compound the challenges of state cybersecurity governance? With anticipated significant disruptions at all spheres of society, the 4IR demands an interrogation of the traditional international law approach to cyber challenges. The horizontal integration of technologies under a 4IR paradigm would potentially carry particularly challenges for policy and governance of state cybersecurity. Policy decisions of states will ultimately determine the social and political disposition of peoples of the world in relation to the development that the 4IR will enable. The philosopher Dooyeweerd aptly remarked that: "[p]erhaps there is no other organized human community whose character has given rise to such a chaotic diversity of opinions in modern social philosophy and social science as the State." (Freeman and de Jongste 1984). Consequently, states need a communal response to the novel capabilities that 4IR technologies will bring. State governance of these technologies, their risks and benefits need to occur in a manner that will protect its populace and preserve the integrity of the state as well as its cyberinfrastructure. The focus of this research is consequently to answer the question, what governance approach should states undertake under international law to produce state cybersecurity governance that is just in the 4IR.

[1] Bitcoin is one of the most famous digital currencies used online. It is also known as cryptocurrencies or e-currencies. It employs a decentralised banking method to record and maintain transactions. The solving of mathematical problems through computational solutions is how new units of the currency is produced.

[2] The employment of the term state cybersecurity governance is deliberate to distinguish it from instances of cyber security governance that involves natural persons. See (European Union 2016). The focus of this chapter is how the state governs its own security in anticipation of the disruptive technologies of the fourth industrial revolution.

Contemporary international law does not yet have a codified response to cybersecurity in general or state cybersecurity in particular. This chapter will proceed by presenting the contemporary international law, state cybersecurity governance approach. The chapter then interrogates the two overarching disruptions that the 4IR will bring to state cybersecurity governance. The methodology that is followed uses the perceived future 4IR disruptions, prominent international law policy documents and the diversity of state practice to discern the prevailing normative order of state cybersecurity governance. The possibility of forms of normative modelling is then postured in order to respond to the primary research question. The chapter concludes by postulating a theory of cyber justice as critical to a 4IR future for states.

2 The Fourth Industrial Revolution and the State

Unlike the previous three industrial revolutions, the 4IR cuts across the globe and holds the potential for equitable development and technological growth. The process advances of the three industrial revolutions differ significantly, not only in the specific technologies convoluting but also in the resulting forms of enterprise and in the nature and role of the actors involved (Colli and Nicoletta 2013). Consequently, predicting the winners and losers is not predicated on the state as a player or even current levels of development of a particular nation. The implications of private individuals affecting the global balance of power will be far-reaching for human development. This withstanding, "[t]he state, however, remains the principal actor in the international arena, and the *raison d'être of the international legal system.*" (Dugard et al. 2011).

The question could be asked, why overarching state intervention is even necessary in a 4IR world of cyberspace. In response, lessons have been learned from the Third Industrial Revolution. Even though states did not play a critical role in the technological expansion of the Internet, but rather private corporate entities—they were critical to the efficiency and dynamical proliferation of this technology. The success of the United States' internet equipment producers is still very dominant globally precisely because they were the early movers in these new high-tech fields (Colli and Nicoletta 2013). Consequently, policy intervention by states in the very early stages of the Third Industrial Revolution meant the difference between success and failure (Colli and Nicoletta 2013).

The advances in technology brought about by the 4IR are focused around three clustered megatrends that exploit the proliferation of digitalization and information

processing power. They are primarily physical,[3] digital[4] and biological[5] (Schwab 2016). Collectively, these technological advances will challenge cybersecurity via their pervasive characteristics. The fundamental characteristics of 4IR technologies that will disrupt the traditional regime of state cybersecurity are four-fold. These characteristics are 1. Interconnectivity; 2. The potential of hyper-communication; 3. uber-intelligence; 4. independent self-learning (Schwab 2016; Groscurth 2018; World Economic Forum 2019). This is not a closed list (*numerus clausus*) of characteristic but is representative of the core challenges that cybersecurity faces. The consequences of this transformed creature on state cybersecurity governance are fundamental disruptions to the traditional functioning of states collective policy response. The pivotal disruptions should be observed on a national level and an international level. Nationally, cybersecurity governance will be disrupted in the manner that it is brought about – via legislative and regulatory processes. Internationally the disruption will challenge the legitimacy of the enforcing state itself, through the notion of cyber sovereignty and the accompanying challenges of jurisdiction. These disruptions are critically interrogated below. The interconnectivity that for example the 'internet of things' technology will produce will fundamentally disrupt state control over cybersecurity protocols. Further, three main factors have been observed in recent years has served as catalysts for the proliferation of 4IR technologies, they are:

1. "Digital components such as sensors, actuators, cameras and microphones nowadays are so small and can be produced so inexpensively that we can use them to teach things to see, hear and feel. By the way, several German producers are leaders in the world market for such products.
2. Since the 2010s, an internationally applicable protocol, IPv6, has existed which enables almost everything to be supplied with its own internet address. This enables a device to establish contact to other devices and people as well as send and receive data.
3. Finally, information science as an engineering discipline has matured and is on the way to become the most important discipline of all. It is used to help networked, sensitive things to act in a sensible and increasingly autonomous manner." (Sendler 2018)

These technological advances have removed much of the control over processes and stakeholders that the state traditionally enjoyed. This produces novel cybersecurity threats for both the state and its citizenry. International law, in turn, has not

[3]The main known examples of these tangible technologies are self-driving or autonomous vehicles, advanced robotics and 3D printing.

[4]The digital revolution will be driven by the interconnectivity of things via what has been described as the 'internet of things'. The internet of things technology will connect the digital worlds with the physical realm.

[5]The advances in computing processing power have opened a door to the biological building blocks of humanity. Consequently, the 4IR allows for a world where human genes can be sequenced, activated and edited.

been able to respond to this new dawn. Consequently, cybersecurity law and governance has not evolved or developed to contend with the challenges of the 4IR. In holding with traditional international law, the objective of state cybersecurity law and governance remains the maintenance of international peace and security. However, the 4IR brings with it a paradigms shift and the developments in human rights law needs to filter through cybersecurity law and governance's notion of justice. In order to secure this objective, state cybersecurity law and governance needs to evolve in order to produce justice under a 4IR paradigm. It is not an understatement that the 4IR could also potentially produce tremendous social inequality. This social disruption will be an added dimension that state cybersecurity governance needs to approach as a potential threat. This threat can also be extended to the conduct of corporate entities and their impact on other states. In regard to this, there is a real likelihood that an organization's plans for implementation of 4IR plans could cause "armed" international disputes (Smith and Pourdehnad 2018). In conclusion, the state remains at the core of the response to the disruption that the 4IR will bring. Consequently, it becomes critical to interrogate cybersecurity governance from the perspective of the state under a 4IR paradigm.

3 State Cybersecurity Governance and International Law

The 4IR developmental challenges of state cybersecurity governance produce fundamental obstacles to the creation of universally accepted norms and standards for states and their cybersecurity. The primary objective of state cybersecurity governance has been the maintenance of international peace and security in accordance with Article 1 (1) of the United Nations (UN) Charter. However, this objective is originally premised on two arcade notions of international law; (1) that the state is the exclusive subject of international law and (2) that the 'use of force' is limited to conventional acts of warfare and/or acts of aggression. In the absence of international consensus on the norms and principles, which are to steer global cybersecurity governance, states have resorted to a proliferation of their offensive cyber capabilities. This is a rational response under a peace and security, international law paradigm for state cybersecurity governance.

Figure 1a, is demonstrative of the global arms race for offensive cyber capabilities, even though some states might argue that their intentions are more defensive. This has divided the globe into two cyber centres of power. A developed world block spearheaded by the United States and are developing world block represented by Russia and China (Fang 2018). How should governance be comprehended by states in terms of executing their cybersecurity policy? The United Nations Development Programme (UNDP) records that:

> Governance is the system of values, policies and institutions by which a society manages its economic, political and social affairs through interactions within and among the state, civil society and private sector. It is the way a society organizes itself to make and implement decisions-achieving mutual understanding, agreement and action.

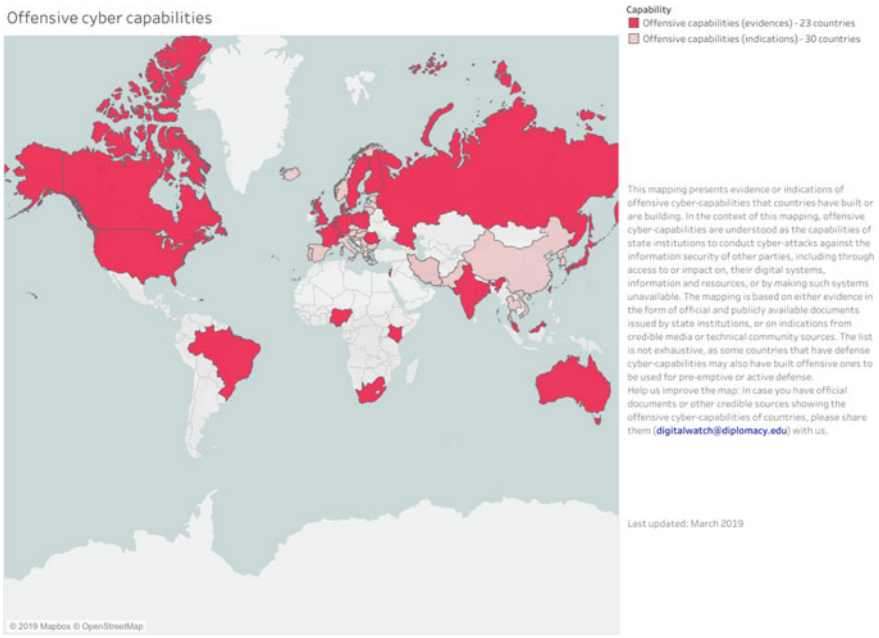

Fig. 1 **a** The global offensive capabilities of states (https://www.diplomacy.edu/cybersecurity)

State cybersecurity governance should have the capacity to accommodate a normative framework, which will be responsive to the challenges of the 4IR. Traditionally, governance is more concerned with the conduct of states rather than their citizenry, but the 4IR produces challenges both with conduct from the state and private citizens. Consequently, through a 4IR paradigm, it is not only states who pose a threat to international peace and security, but private citizens too. Cyber acts of aggression by private citizens of a particular state could easily fit the mould of 'use of force' in order for another state to proffer a justification for its own aggression. It has been argued that even though Article 2 (4) of the UN Charter prohibits 'use of force' by states and broadening the definition of 'use of force' to include private citizens could assist international law (Kulesza 2009), this is not the position in international law as yet. However, a cyber-crime or -attack, in essence, could be construed as the use of force against the political and economic interest of a state or its citizenry. Though states generally struggle with these definitions in developing domestic legal instruments. For example, that "a cyber-crime is a broad concept analytically distinct from cyber-attack. While, as with the concept of cyber-attack, there is no universally recognized definition of cyber-crime (Hathaway 2012)."

International law further lacks consensus where the cyber conduct of a private individual rises to an act of aggression against a state and such action benefits that person's own state. However, it would be possible to attach liability for the conduct of a private person or groups of people to a state via the international law concept

of state responsibility. This will require proof that the state had 'effective control' over the perpetrator of a cyber-attack. So also, the traditional international law test of 'effective control' in order to a tribute state responsibility to the conduct of an individual will need rethinking. The International Court of Justice (ICJ) produced this test by stating:

> State's responsibility can be incurred for acts committed by persons or groups of persons—neither state organs nor to be equated with such organs—only if, assuming those acts to be internationally wrongful, they are attributable to it under the rule of customary international law reflected in article 8 [of the ILC's draft articles].[6]

Under this definition, international law does provide for a degree of accountability where a private person or group of people, but only at the direction and control of a state executes a cyber-attack. State cybersecurity law and governance need to develop in a manner that is more human-centred and allows for liability inclusive of a developed view of the subjects of international law. Especially because state cybersecurity law and governance resides at the heart of our 4IR future. The maintenance of the rule of law and efficiently articulating state responsibility under a 4IR paradigm will be the core functions of state cybersecurity law. However, international law would first have to resolve the primary issue of a definition of cybersecurity. Internationally cybersecurity remains beset with the challenge of its own definition (Kosseff 2017). Kosseff (2017) ventures a definition in that:

> [C]ybersecurity law promotes the confidentiality, integrity, and availability of public and private information, systems, and networks, through the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security.

This definition allows for a progressive perspective of cybersecurity law that embraces a 4IR paradigm. However, cybersecurity law and governance would need to develop legal norms and principles that also capture ever-evolving forms of cyber-attacks and still maintain the rule of law and the protection of human rights. In addition to this, cybersecurity needs to develop beyond the notion of protecting the infiltration of a secure computer network or critical infrastructure, to include for example 4IR cyber threats. From contemporary examples, these include the distributed denial of service attacks and planting inaccurate information (Hathaway 2012). The accessibility and technological equality that 4IR will produce allows for these normal threats. The underdeveloped nature of international cybersecurity law and policy presents a fundamental challenge to the attainment of a universally accepted state cybersecurity governance regime with accepted norms and principles.

In presenting the question, whether the international law of cybersecurity is in crisis Macak (2016) identifies three apparent crisis indicators. First, the area of cybersecurity appears resistant to the codification of the applicable rules in a comprehensive multilateral binding treaty. Secondly, Macak (2016) observes that "states have

[6]Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), ICJ Rep 2007, para. 406. See also Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. USA) ICJ Rep 1986, paras. 109 and 115.

shown extreme reluctance to contribute towards the development of cyber-specific customary international rules." Finally, Macak (2016) remarks that:

> … the third concerns their (*states*) actual conduct in relation to cyber governance. It would be inaccurate to claim that states have entirely given up on standard-setting. However, instead of interpreting or developing rules of international law, state representatives have sought refuge in the vacuous term 'norms'.

The crisis or criticism that Macak (2016) remarks on is the pluralization of international norm-making (Berman 2007; Aspremont 2012). Objective observation suggests that one has to side with Macak (2016) on the first two crisis indicators. However, what Macak (2016) does not observe is that the rationale for the third crisis indicator resides within the first two. It is due to the inability of states to produce a consolidated legislative and regulatory regime for state cybersecurity law and governance, that the approach of norm-setting is justifiable. Further, the challenge of codification is even more insidious on a domestic level with fears of government controlling the personal data of its citizens (Janssen and van den Hoven 2015). The development of norms seems to be the only manner of reaching some sort of international consensus for cybersecurity law and governance.

Where states have developed domestic legislation to regulate cybersecurity law and governance, one could discern customary international law from such State practice. However, international law requires that such State practice needs to be both extensive and uniform amongst states. In the North Sea Continental Shelf cases, the ICJ held that:

> An indispensable requirement would be that within the period question, short though it might be, state practice, including that of states whose interest are especially affected, should have been both extensive and virtually uniform in the sense of the provision invoked; and should moreover have occurred in such a way as to show a general recognition that a rule of law or legal obligation is involved…

Consequently, state practice has not been consistent in order to produce customary international law rules because the subject matter and challenges of such rules vary from state to state. It is critical to the integrity of international law that the distinction between current law (*lex lata)* and future law (*lex ferenda)* be maintained. The ICJ has been consistent in confirming that current law or positive law is the starting point for all judicial inquiry. Thus through the application of international law, the legal scholar needs first to establish what the law is before it can delft into what the law ought to be. The purpose of this is not to favour one norm over another, but to foster their relationships. In the *Islands of Palmas case*,[7] the arbitrator Max Huber remarked that international law "… has the object of assuring the co-existence of different interests which are worthy of legal protection." Consequently, a normative approach to state cybersecurity law and governance would not only serve to produce an international regime but also lead the way towards international state consensus.

[7] *Island of Palmas Case (or Miangas), United States v Netherlands, Award* (1928) II RIAA 829.

4 State Cybersecurity Governance Under a Disruptive Fourth Industrial Revolution 4IR Paradigm

4.1 The Future of Legislative and Regulatory Regimes

The process of law and policy-making on cyber-related matters is primarily legislative within domestic legal orders. At present international law does not have a legislator for all states. This has produced a plurality of competing and equivalent legal sources, both within domestic jurisdictions and in international law. International lawyers find solace in the prescripts of Article 38 of the ICJ Statute in order to have some remnants of legislative order for retrieving international law. Article 38 of the 1945 ICJ Statute provides for a hierarchy of legal sources starting with treaty law, customary law, and general principles. These are then complemented by other sources usually deemed as ancillary they are case law and the writings of eminent experts in the field of law (Teitel 2013; Chirwa and Chenwi 2016). In a 4IR world that is fast-paced; interconnected; autonomous and self-learning, the slow turning wheels of legislative bureaucracy stand in stark contrast. The production of laws and policies would be unable to keep pace with the rate of technological change. Where constant law-making becomes the response to the fast pace development in 4IR technologies, the result would be the fragmentation of an already fragile international state cybersecurity regime. Legislative intervention is a response, would also be further exacerbated through the horizontal integration of 4IR technologies both globally and municipally.

Consequently, what is needed is "a set of higher normative essentials that guides the governance and application of existing laws (Michelman 1995)." The challenge for the future of the legislative and regulatory regimes of state cybersecurity governance would be the development of higher norms, similar to constitutional principles under a constitutional democracy. The 4IR will challenge the "character of security threats while also influencing shifts of power, which are occurring both geographically, and from state to non-state actors (Schwab 2016)." This presents a further challenge to a legislative and regulatory approach as a solution. States would have to develop laws for technologies that they do not understand and which is operated from stables of power that they cannot identify. Schwab (2016) observes that the "critical danger is that a hyper-connected world of rising inequality may lead to increased fragmentation, segregation and social unrest, which in turn creates the conditions for violent extremism." Developing guiding and essential norms for all states will produce a safeguard against the rapid pace of technological development in the 4IR. International law would then not need to usurp the legislative functions of states through codification but will only be responsible for norm-setting. Such a normative approach will be consistent with contemporary international law in that it still premised on state consent and free will. In the *Lotus Case*[8] judgement the ICJ proclaimed the position of international law in that:

[8] *The Lotus Case* (France v. Turkey), PCIJ Reports, Series A, No. 10 1927, 18.

> The rules of law binding upon States, therefore, emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims.

A normative approach would also allow for legal certainty. Private actors would consequently follow the same set of higher norms that the state follows. What is certain about the future viewed through a 4IR lens is that only a multi-stakeholder, collective approach towards progress can ensure justice and the integrity of the state. The smart solutions and responses to the challenges of the 4IR will not be provided by a singular state or leader. However, by adopting novel leadership concepts, rather than responding via legislation, which can become arcade during the process of its enactment, stakeholders can adequately respond to the technological disruptions of the 4IR. Working together, both locally and globally states and production leaders from numerous businesses such as start-ups, large companies and labour can develop much more efficient solutions to these disruptions brought about by the 4IR. Kennedy aptly reminds one that:

> Any so-called 'realism' that attends only to the overt acts of national sovereigns is no longer realistic. In our world, power lies in the capillaries of social and economic life. Myriad networks of citizens, commercial interests, civic organisations and government officials are more significant than interstate diplomacy. Statesmen and stateswomen act against a background fabric of expectations—the legitimating or de-legitimating gaze of world public opinion—and they act in the shadow of all manner of public and private norms.

Where the state follows the path of norm development, one has to guard against supranational institutions following the path of legislating international law for state cybersecurity. The legitimacy of international law depends critically on the institutions of international law to be also legitimate. Where legislative or rulemaking functions are embedded in global governance institutions outside of the democratic system of the national state, this compromises the legitimacy of international law. What we have seen with global governance institutions such as the World Trade Organisation, the UN Security Council, the World Bank and even the European Union; is enduring patterns of coordinated, organised and persistent rulemaking governance. Global governance institutions, "though created and sustained through treaties made by states, are increasingly taking on lawmaking functions (Besson and Tasioulas 2010)." The sovereignty of states could potentially be compromised where we do not protect its integrity.

4.2 The Ascend of Cyber Sovereignty

State sovereignty is a keystone principle of international law (Benvenisti 2013; Alvik 2011). Cyber sovereignty can be interpreted in two ways. The first is cyber sovereignty as "a natural extension of national or state sovereignty in cyberspace (Fang 2018)." Cyber sovereignty is consequently directly linked with territorial

integrity, as it is comprehended in international law. This view supports and has as its main content the state's authority to exercise jurisdiction in cyberspace (Fang 2018). The second is cyber sovereignty as an external quasi-geographical global cyberspace, which is boundary-less and encompasses an all-inclusive international jurisdiction of the global cyberspace. This second hypothesis is much more consistent with the notion of the 4IR. However, under the first hypothesis, cyber sovereignty follows the traditional tenants of state sovereignty. The principle of cyber sovereignty is lamented with traditional international law principles such as "equality among nations and the principle of non-interference in other nations' internal affairs and by implication also each other's cyberspace (Fang 2018)." Defining cyber sovereignty outside of the traditional notions of state sovereignty would mean that states will lose much of the exclusive authority and dominium, they currently enjoy over the domestic activities in cyberspace. It has been observed that for "superpowers such as the United States, China and Russia it is of critical importance to define cyber sovereignty to be consistent with the notion of state sovereignty (Fang 2018)."

Traditionally, international law perceives state sovereignty to be integrally linked to the territorial integrity and political independence of a state (Besson and Tasioulas 2010). However, in a 4IR world, states will become much more interconnected and dependent on each other both politically and economically. Is it then possible for sovereignty to accommodate both independence and interdependence of states? In the *Islands of Palmas-case*, it was noted that sovereignty means "[i]ndependence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State." From this position, the arbitrator Max Huber seems to suggest that the functioning of a state's sovereignty links critically to its independence. The normative order of international law is inherently dependent on this nature of statehood. The implications for state cybersecurity law and policy is paradoxical. The *Lotus Case* went on to confirm that "[n]ow the first and foremost restriction imposed by international law upon a State is that-failing the existence of a permissive rule to the contrary, it may not exercise its power in any form in the territory of another State." The very nature of state sovereignty seems to be challenged by the notion of cyber sovereignty.

The second hypothesis of cyber sovereignty seeks to disrupt the traditional notion of state sovereignty in cyberspace. This notion of sovereignty is not wholly inconsistent with the origins of sovereignty as it emanates from the transfer of an individual's autonomy to a collective, represented by the state. The legal theorist De Vattel (2011) commented that:

> … sovereignty is that public authority which commands in civil society, and orders and directs what each citizen is to perform, to obtain the end of its institution. This authority originally and essentially belonged to the body of the society, to which each member submitted, and ceded his natural right of conducting himself in everything as he pleased, according to the dictates of his own understanding, and of doing himself justice."

The notion of sovereignty is consequently linked with that of cyber justice. The concept of sovereignty presents a unique dichotomy for state cybersecurity governance under a disruptive 4IR paradigm. States in favour of the 4IR developments

who seek to control systems and networks will use cyber sovereignty as a justification under the first hypothesis. On the other side, States who lag behind of fear the change will employ protectionism and nationalism to insulate their citizenry from 4IR disruptions. We have already observed this with states like the United States, with the rise of popular nationalism (Bonikowski and DiMaggio 2016). These States too will justify their decisions under the banner of cyber sovereignty. The concerns around the disruptions of the 4IR should not wholly be dismissed, because popular fear holds the potential of derailing the potential benefits of 4IR technologies. Goldring (1998) correctly warns that:

> "If a majority of voters in some countries feel that their political sovereignty is threatened by the free play of market forces, they are right. It is a characteristic of national sovereignty that nations can choose whether to submit to the interests of free trade and transnational business or not. Their choice need not be rational."

Cyber sovereignty needs to be defined and applied in a manner that produces justice for the individual citizen. Although, international law is not overly interested in the political tools of democratic control it is critical to incorporate notions of democratic legitimacy and its processes, in particular where it intrudes into national law. In the "probably most characteristic example, the ICJ did not decide, in its *Advisory Opinion on the Threat or Use of Nuclear Weapons*, on the question of whether the state interest or humanitarian principles prevail when in conflict with each other. The then ICJ President Bedjaoui created the category of 'neither allowed nor forbidden' for a clash between state and individual values."[9] However, international law would have to be much more decisive in terms of which hypothesis of cybersecurity prevails. What is critical is that whichever notion of cybersecurity international law adopts it needs to produce justice in order to maintain international peace and security in cyberspace.

4.3 Justice Disrupted

The ultimate normative order that international law proffers under a 4IR paradigm, would need to be conscientious of the advances in human rights in order to protect individual liberties in cyberspace and produce justice as an objective and as an outcome. As demonstrated above, following a regulatory or legislative approach domestically would also eventually just result in fragmentation of the international law regime. The objective of justice has been overlooked in the development of cybersecurity law and governance. The primary focus of states has been related to questions around adjudication and jurisdiction. This has usurped the objective of justice (Dekker and Werner 2004). State cybersecurity governance needs to develop policy objectives that link directly to established notions of justice. This should be open to an objective test such as, "suppose we say that, to justify directly a political

[9] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 ICJ Rep, 226.

act is to show the correspondence of this very act (not just some higher-level act that authorized this one) to ideals of justice or conduciveness to general human goods (Michelman 1995)." In order to govern the disruptions of the 4IR in a stable manner, state cybersecurity governance needs to be evolve inclusive of justice. Mihr (2016) ventures a working definition of cyber justice that is:

> … based on good cyber governance and its human rights-based approach for (1) more accountability, (2) more transparency, and (3) more participation by multiple stakeholders and actors through the use of cyber tools, such as the Internet and other mobile devices.

The definition of cyber justice in itself holds normative characteristics to guide state cybersecurity governance. Consequently, state cybersecurity governance will achieve justice by adopting the normative tenants presented by cyber justice. These norms are accountability to the general populace, transparency, openness or flexibility to multi-stakeholder participation. These normative tenants will allow resilience in order to manage the disruptions of the 4IR and potentially avoid violent international conflicts between States. International law generally, suffers from the trauma of world wars as the fundamental rationale to its legal development. This is the rationale for the maintenance of peace and security as the primary objective in international security and consequently for state cybersecurity. An evolved objective for state cybersecurity under 4IR paradigms should be cyber justice.

5 The Fourth Industrial Revolution as Cyber Justice

States will in effect have two choices in determining how to respond to the challenges and potential international conflicts that the 4IR will produce for state cybersecurity governance. States can either follow a 'to war/law of war' (*jus in bello/ad bellum) a*pproach or a cyber justice approach. The notion of cyber justice presents a normative foundation for managing the degree of disruption that 4IR technologies will produce. Weil (1983) remarks that "the capacity of the international legal order to attain the objectives it was set up for will largely depend on the quality of its constituent norms." International law needs to be decisive and place at the centre of its normative order the foundational notion of cyber justice. However, these norms do not and cannot automatically offset the sovereignty of a state (Weil 1983). Jayasuriya (2001) argues that:

> As law and the territorial state are uncoupled, power of governance is becoming increasingly fragmented and diffused within the market and civil society; this poses an immense challenge to the traditional antinomies—between legality and legitimacy as well as between sovereignty and society—that underpinned the 'government' model of sovereignty.

The hypothesis of cyber sovereignty discussed above is consistent with a 4IR future. This view of cyber sovereignty will primarily be responsible for the uncoupling of the state power of governance in cyberspace. This is where the state leaders agree with this assertion not (Fang 2018). In order for the contemporary international

order to hold, the governance of state cybersecurity needs to elevate itself to a set of higher legal norms. These higher legal norms need to find broad collective consensus amongst states, but they also need the recognition of all the players in cyberspace. The notion of cyber justice is but only one such normative foundation. However, it presents a valiant opportunity for the preservation of the state and its central function of protecting its citizenry against threats in cyberspace. Where states would want to impose the rule of law in cyberspace based on the traditional notions of sovereignty and international law, they would proceed at their own peril.

6 International Cooperation and Mutual Assistance as the Existing Normative Order for State Cybersecurity Governance

6.1 Background: The Objectives for State Cybersecurity Governance

Even though it can be argued that no consolidated or codified international legal order exists for state cybersecurity governance, an argument can be made for the presence of a normative order that is predicated by the objectives of international law. Kelsen's (1961) statement that "[t]he legal order is a system of norms", finds particular application for state cybersecurity governance under international law. International law is focused on three objectives in developing state cybersecurity governance protocols. The primary objective is the maintenance of international peace and security, the second is the harmonisation of legislative frameworks and thirdly cooperation amongst states. All three of these objectives face disruptive challenges under a 4IR paradigm. However, international cooperation and mutual assistance seem to have been elevated as a norm in state cybersecurity policy. It is problematic that the interpretation and application of the notion of international peace and security are premised on resolving cyber threats by applying the mechanisms and thinking of conventional warfare. The technological advances of the 4IR will produce novel surreptitious threats and clandestine perpetrators. As shown above the objective of the harmonisation of legislative frameworks, in itself would be challenged by the slow-pace of bureaucratic mechanisms relative to the swiftness of 4IR technologies.

However, international cooperation and mutual assistance seem to have filtered through in the majority of international state cybersecurity policy propositions. International cooperation and mutual assistance as an aspiration are challenged by the contemporary inequalities already existing between states. International law does not at the moment have a consolidated state cybersecurity governance regulatory framework or legal principles that are recognised by the majority of states. In the absence, of such governance infrastructure, individual states might be tempted to follow a 'to war/law of war' approach to resolve threats or attacks against their cybersecurity. Grotius said, on the idea of 'just war' when in the face of a multiplicity of sovereigns:

> I observed that men rush to arms for slight causes, or no cause at all, and that when arms have once been taken up there is no longer any respect for law, divine or human; it is as if, in accordance with a general decree, frenzy had openly been let loose for the committing of all crimes. (Grotius 1925)

Although it is accepted, that there is "no single path to war and peace but multiple possibilities (Marwala and Monica 2011)." The application of the 'to war/law of war' approach to incidents of breaches in states cybersecurity could have disastrous effects for the maintenance of international peace and security, especially where a private individual is involved. Currently, under the 'to war/law of war' approach, there are three incidents or categories of individuals which a state can lawfully target; these "are combatants, civilians directly participating in hostilities, and civilians acting in a continuous combat function (Iyi 2016; Gill et al. 2014; von Heinegg 2014)." However, it is clear how the law of war approach to cyber-attacks; cybercrime's or cyber-warfare could be apocalyptic in a world with nuclear capacity. The traditional notion of going to war or declaring war does not apply under a 4IR paradigm. Cyber-warfare is much more fluid, the participant more obscure and the interest or motives greatly variant.

The methodology followed below is to present the key international and regional policy documents that in essence have already produced an international normative order for state cybersecurity governance. The key norm that the majority of these policy interventions have produced is that of international cooperation and mutual assistance.

6.2 UNGGE Report

The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE)[10] released its third report in 2015. The Group emphasized "the importance of international law, the Charter of the United Nations and the principle of sovereignty as the basis for increased security in the use of Information Communication Technologies (ICTs) by States (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015)." The UNGGE report did an analysis of existing and emerging threats and concluded that generally there is been a proliferation of malicious use of ICTs globally. These increased threats perpetrated by both non-state and state actors pose significant challenges to the maintenance of international peace and security. The advent of 4IR technologies will increase the capacity of the malicious use of ICTs. The UNGGE report identifies that "the most harmful attacks using ICTs are those directed against a state's critical infrastructure and the communication and information systems linked to them."

[10]The UNGGE was established through the UN General Assembly resolution 68/243.

In the threat analysis of the UNGGE report, the panel identifies a novel threat to international peace and security. The report recognises that there has been an increase in non-State actors perpetrating malicious attacks indirectly against a States. What makes the emergence of these new non-state actors particularly challenging is that they are; firstly, diverse in their make-up and motive;[11] secondly the speed with which they execute malicious attacks; thirdly the challenge of establishing the source or the origin of incidents. The focus of these attacks is producing destabilising misperceptions and inciting conflict and harm to the citizenry. One can imagine a future where AI potentially could be developed and deployed to execute such attacks. In effect, the citizenry of state can be manipulated into a weapon against that state itself. The UNGGE report improves "the security of critical ICT infrastructure; develop technical skills and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use (UNGGE 2015)."

Although the UNGGE failed to produce binding international law, it did show that the norm of international cooperation and mutual assistance was generally accepted by all states. The report proposes as a solution "[v]oluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability." Unfortunately, the UNGGE could not produce consensus amongst member states and what followed was the development and adoption of two new resolutions. One was sponsored by the European Union, with the involvement of states such as Japan, the United States, Australia and Canada. In essence, creating a completely new group of government experts. The second resolution created an Open-Ended Working Group (OEWG) under the auspices of the UN. The second resolution was primarily sponsored by China and Russia together with African and Asian countries. The OEWG focuses on, the development of international law rules, norms and principles for how states should deal with cybersecurity. Although international cooperation and mutual assistance presented itself under two centres of power, it was the only surviving consensus from the UNGGE.

6.3 Budapest Cybercrime Convention

The Council of Europe produced the Convention on cybercrime or as it's properly known 'the Budapest Convention' in 2001 and it entered into force on 1 July 2004 (Council of Europe 2004). Although the focus of the convention is cybercrime, it does produce norms for international law that would be directly applicable to state cybersecurity governance under a 4IR paradigm. With five ratifications, the Budapest Convention is known as the only binding multilateral international law instrument on cybercrime (Clough 2014). The convention seeks to serve as a framework or model

[11] These non-state actors, consists of terrorists, criminal groups as well as individuals operating independently.

law for the enactment of domestic laws that holds international cooperation at its core.

The convention provides for international cooperation and mutual assistance through allowing for multi-stakeholder involvement in the combating of cyber-crimes, by recognising corporate entities together with natural persons. This is consistent with the notion of cyber justice that advocates for accountability, transparency and participation.

The staggered adoption of the Budapest Convention is evidence of the fallacy of international harmonisation of laws. This supports the argument for a normative approach to developing international law and norms for state cybersecurity, rather than enacting more legislation or regulations. There is been a debate around the manner in which international cooperation and mutual assistance should be developed, following the Budapest Convention. However, "the binary debate about the convention versus a UN convention in some way presents a false dichotomy (Clough 2014)." Where states are required to respond to their national security, the self-interest produced by state sovereignty will always move decision-making inwards. Consequently, "each country will determine what it considers necessary to effectively combat cybercrime, looking to national, regional and international standards in enacting laws that best suit its national circumstances (Clough 2014)."

6.4 NATO Tallinn Manual

International cooperation and mutual assistance as a norm probably find its greatest perversion through the Tallinn Manual. The 'to war/law of war' approach is probably best expressed through the perspective adopted by the North Atlantic Treaty Organisation (NATO) via its Tallinn Manual. The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), based in Tallinn, Estonia embarked on a research project in 2009 in order to produce international law's most comprehensive body of work on cyber warfare. The majority of cyber-attacks or cyber-crimes does not satisfy the international law requirements for 'the use of force' under the prescripts of *jus ad bellum* and *the jus in bello* (von Heinegg 2014). Although the Tallinn Manual does recognise international cooperation and mutual assistance as its core consensus, promising the development of a normative framework towards cyber justice is more consistent with contemporary international law than a 'to war/law of war' approach. The Tallinn Manual is focused on inter-state relations and approaches state cybersecurity from the perspective of public international law (von Heinegg 2014). Consequently, under a 4IR paradigm, the Tallinn Manual does not accurately keep pace with evolving realities of state cybersecurity law or governance. von Heinegg (2014) correctly criticises the manual for its almost exclusive analysis of the 'to war/law of war' approach.

6.5 SADC Model Law: Computer Crime and Cybercrime

In the African context, international cooperation and mutual assistance have found a direct application through the work of the Southern Africa Development Community (SADC). SADC has been consistent in its approach to see cybersecurity as a public security sector threat. Consequently, cybercrime is identified as a challenge under public security by SADC's Directorate Organ on Politics, Defence and Security. This is consistent with the notion of cyber justice. This approach produces a particular challenge for the development of normative standards for state cybersecurity governance in order to effectively and efficiently respond to disruptions brought about by the 4IR. However, SADC has traditionally followed the prescripts of developed international law. The approach in Southern Africa, through the endeavours of the SADC to achieve the three objectives of state cybersecurity governance, was the development of a model law. The norm, international cooperation and mutual assistance find a procedural application through SADC's model law. The SADC normative approach involves the harmonisation of state cybersecurity policy, through the 'establishment of harmonised policies for the ICT market in the Group of African, Caribbean and Pacific states (ACP) countries' (SADC 2013).

7 Normative Modelling for Fourth Industrial Revolution State Cybersecurity Governance

State cybersecurity governance for the 4IR needs to be developed through an evolved notion of cyber justice. Such 4IR normative modelling of state cybersecurity governance underpinned by cyber justice cannot be a closed list *(numerus clausus)* of policy suggestions but must be open to other governance norms and principles. These include governance principles viewed as good, cooperative, analytical in the outcome, future-forward and adaptive. The achievement of cyber justice would mean that these norms are reconcilable with norms such as the respect for human rights, accountability, transparency and participation. How these norms function and their relationships within a system of governance should be consistent with the legal system. In order for a norm to belong to a system, it needs to demonstrate connectivity or a rational validity, which traces that norm back to a base norm. The connectivity can manifest through an assumption of truth borne from objective experience or the immediately observable reality (Kelsen 1961). Various governance models have been developed in the past, each of which adopts characteristics that could produce cyber justice. Consequently, it is important to briefly discuss these models and their reconcilability with cyber justice.

7.1 The Continued Relevance of Good Governance?

The political, economic and social governance of a state is consequently an inclusive approach. What is envisioned for state cybersecurity governance is not only governance on a political, economic, social and cyber front, but also the cross interaction between these spheres. What follows is the question, how does one then measure the achievement of these objectives around in policy? Generally, the common policy yardstick towards which the international community aspire to is good governance. Consequently, what is good governance? The UN General Assembly confirmed through the famous Resolution 66/288 "The Future We Want" that good governance is a cornerstone for development. This would be inclusive of state cybersecurity governance for 4IR development. UN Resolution 66/288 states:

> Democracy, good governance and the rule of law at the national and international levels, as well as an enabling environment, are essential for sustainable development including sustained and inclusive economic growth, social development, environmental protection and the eradication of poverty and hunger.

Good governance is consequently founded on principles such as participation, populace voice, direction, performance, accountability and fairness. These principles postulates that good governance is where all people affected should be part of decision-making through credible institutions. Good governance focuses on broad consensus in order to achieve the best interest of peoples through policies and the procedures to effect such (Kriangsak 2017). State cybersecurity governance directed towards the strategic vision of good governance involving all affected stakeholders would be consistent with the theory of cyber justice. Good governance further holds a long-term perspective directed towards human development and drives government, the private sector and the public at large. This should be understood as inclusive of a collective understanding of what is needed to achieve good governance. Consequently, through its definition, good governance demands an awareness of the socio-economic, historical, cultural and political nodes that shape a community or state.

Performance as a principle of good governance is more focused on the institutional dynamics that underpin good governance. The principle demands institutional responsiveness through their processes. It further seeks the cultivation of a non-discriminatory institutional culture in servicing all affected parties. Together with this, the principle of performance would endeavours to achieve the best utilisation of cybersecurity resources through being effective and efficient.

The principle of accountability premises good governance on the need for decision-making parties to be accountable to all stakeholders, especially the affected public. The nature of the decision would obviously affect the nature of accountability. Central to this principle is the institutionalisation of transparency. Transparency premised on the access to information, institutions and due process for concerned parties. This access should be strengthened through support that assists better comprehension of information and monitoring of it.

The last principle of good governance is fairness. Fairness is pillared by two sub-principles being equity and the rule of law. Good governance should consequently be interpreted as firstly, equal opportunity amongst states towards their development under a 4IR paradigm. Secondly, good governance postulates that under the rule of law all legal frameworks should be fair and their implementation should impartial. It is clear from the above that good governance is not only consistent with the notion of cyber justice but a necessary accompaniment for 4IR state cybersecurity governance.

7.2 Cooperative Governance

The prevailing contemporary international law norm of international cooperation and mutual assistance needs to be developed for state cybersecurity governance. International cooperation viewed under liberal theory presents a causal path between economic interdependence and interstate wars (Marwala and Lagazio 2011). The more states depend on each other economically it should reduce the risk of following a 'to war/law of war' approach and rather embrace cooperative state cybersecurity governance. This approach will also find support through the notion of cyber justice. The fundamental idea of cooperative governance in state cybersecurity needs to transform under a 4IR paradigm, from a state-centred idea to a broader inclusive governance model. Schwab (2016) notes that "it is, therefore, critical that we invest attention and energy in multi-stakeholder cooperation across academic, social, political, national and industry boundaries." Cooperative governance also played a critical role in developments within the Third Industrial Revolution. The recognition of multi-stakeholders by governments and involving them in policy development assisted the advances within the telecommunications software industries. Consequently, it is reasonable to argue that science policy, technology policy, and intellectual property rights policy have been crucial during the Third Industrial Revolution (Colli and Nicoletta 2013).

International law can learn from its past in the manner that international cooperation and mutual assistance consensus that led to binding international law. Article 11 of the Moon Treaty states "The moon and its natural resources are the common heritage of mankind, which finds its expression in the provisions of this Agreement, in particular in paragraph 5 of this article."[12] Paragraph 5 expresses a commitment by:

> States Parties to this Agreement hereby undertake to establish an international regime, including appropriate procedures, to govern the exploitation of the natural resources of the moon as such exploitation is about to become feasible. (United Nations 1979)

The paragraph further expresses that the common heritage of mankind is a doctrine clearly developed as an anticipatory measure to produce a new form of international

[12] Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, Dec. 5, 1979, 1363 U.N.T.S. 3.

cooperation. This measure is born from a period of international conflict and developments in science, which necessitated an increased awareness of the environment and our relationship with it. So too in this period of technological advancement and with the knowledge of the disrupted future, international cooperation and mutual assistance would assist in not only managing the transition but producing cyber justice and legal certainty.

7.3 Analytical Outcome Governance

State cybersecurity governance has much to benefit from the discipline of policy statistical analytics in order to achieve cyber justice as an outcome. Analytical outcome governance will assist states to manage the degree of disruption preemptively rather than reactively. The introduction of analytical outcome governance into state cybersecurity brings with it the capacity for policy analysis which is more focused and involves competencies and capabilities as well as effective knowledge acquisition and utilisation of the processes of policies (Howlett 2018). A primary characteristic of the 4IR is the availability of enormous amounts of basic data. With cyber justice as the prescriptive objective, introducing analytical capacity into state cybersecurity governance will allow for interventions that are more precise. Decision-making outside of an analysis of these sets of data would naturally place a state at a disadvantaged position relative to other states. Consequently, analytical outcome governance is a crucial prescriptive characteristic for 4IR state cybersecurity governance. Howlett (2018) finds that "governments, as a whole, exhibit an uneven distribution of capacities, technical capabilities, and utilization practices across different organizational and thematic venues." In order to achieve success with the introduction of analytical outcome governance, safeguards need to be introduced. Analytical outcome governance needs to have transparency and depressed protection of the right to privacy at its core, consistent with the prescripts of cyber justice. This would involve the decentralisation of state cybersecurity governance mechanisms and retraining state cybersecurity governance officials (Vyas 2018). Such an approach would be consistent with both cyber justice and the accepted theory of cyber sovereignty above.

7.4 Future-Forward Governance

State cybersecurity governance in the 4IR would need to keep pace with the ever-fleeting and expanding set of technologies such as machine learning and artificial intelligence. As one is reading this chapter without a doubt high-velocity advancements in robotics, automation, digital transformation, artificial intelligence, and 3-D printing have considerably advanced (Groscurth 2018). In order to be equal to the challenges and disruptions brought about by the 4IR, state cybersecurity

governance needs effective leadership. Such leadership needs to be embedded in the normative framework of state cybersecurity governance in order to produce future-forward thinking or smart, connected leadership (Groscurth 2018). Groscurth (2018) postulates that smart, connected leadership has—at its core—five fundamental demands: presence, agility, collaboration, development, and discernment. Without future-forward governance, indiscriminate 4IR technology will lead the world into the future and not the inverse. In terms of the values that future-forward governance underpins, it does hold the potential to be reconcilable with cyber justice in its outcomes.

7.5 Adaptive Governance

State cybersecurity governance, which is adaptive, would also need to be responsive in order to achieve cyber justice as an outcome. Including the potential for adaptation into the normative modelling of state cybersecurity governance will introduce flexibility and resilience into the regime. Noting the characteristics of 4IR technologies and especially the pace of change that these technologies are capable of, state cybersecurity governance needs to be flexible through adequately responding to their potential disruptions. Adaptive governance for the 4IR includes and requires adaptive leadership (Weiler 2001). This means, "with the high speed of change, the challenge for leaders is learning faster than the world around them changes. To ensure success, leaders may need to abandon old behaviours, habits and beliefs, only keeping those that best serve them and their people (World Economic Forum 2019)." In the case of adaptive governance, cyber justice would best serve as the conscience for states and their policymakers.

8 Conclusion

The research question was what policy approach should states undertake under international law to produce state cybersecurity governance that is just in the 4IR? This was underpinned by a hypothesis that accepted that the 4IR would disrupt state cybersecurity governance in two ways. The first is that the traditional mechanisms for intervention, which are legislative and/or regulative responses, will be rendered ineffective and redundant at worst. The second was that the 4IR would challenge traditional notions of sovereignty and by implication statehood, through what has been termed cyber sovereignty. The theory of cyber justice is advanced to answer the research question and to serve as an equitable and objective norm-setting approach to state cybersecurity governance. The presence of cyber justice in the development of state cybersecurity governance would mean good cyber governance that is premised on a human rights-based approach, with more accountability, greater transparency and broad multi-stakeholder participation.

This research has sought to make a broad argument for a developmental shift in international law's approach to state cybersecurity governance. The potential 4IR disruptions to state cybersecurity governance demand a change in focus for the adequate development of state cybersecurity. It is conceivable future, that for state cybersecurity governance these disruptions will hit at the core of the integrity of the state as well as render ineffective our customary legislative and regulatory interventions to legal challenges. This shift needs to happen from an international law perspective on the maintenance of peace and security towards the achievement of cyber justice. This precipitates and needs to adopt a normative approach to state cybersecurity governance, rather than a legal positivist approach. The consensus would be easier to reach around norms and principles for state cybersecurity governance in particular and international cybersecurity law in general. Once such consensus has already been achieved through the norm of international cooperation and mutual assistance. Following traditional international law, it can be said that through this development in state practice generally in future international cooperation and mutual assistance has risen to become a general principle of customary international law.

The 4IR is forging a path for the fast pace of technological development and the rapid disruptions to our traditional notions of how the world functions. The law and legal principles as the organizing structure to human development will not be spared. The global order is already experiencing a proliferation in protectionism and nationalism to guard against these disruptions. However, states cannot develop in isolation and an inwards retraction would produce domestic security instabilities. State cybersecurity governance for the 4IR should be pliable enough to accommodate normative standards such as international cooperation and mutual assistance as well as cyber justice.

Acknowledgements This paper is part of activities, assistance and incentives provided at the University of Johannesburg to be at the vanguard of research involving the 4IR. The assistance and patience of Mallissa Lenong have also been invaluable.

References

Alvik I (2011) Contracting with sovereignty: state contracts and international arbitration. Studies in international law, vol 31. Hart Pub, Oxford, Portland, Or

Aspremont J (2012) From a pluralization of international norm-making processes to a pluralization of the concept of international law. In: Informal international lawmaking. Oxford University Press, pp 185–199. https://hdl.handle.net/11245/1.378436

Benvenisti E (2013) Sovereigns as trustees of humanity: on the accountability of states to foreign stakeholders. Am J Int Law 107(2):295. https://doi.org/10.5305/amerjintelaw.107.2.0295

Berman PS (2007) A pluralist approach to international law. Yale J Int Law 32:301

Besson S, Tasioulas J (eds) (2010) The philosophy of international law. Oxford Univ. Press, Oxford

Bonikowski B, DiMaggio P (2016) Varieties of American popular nationalism. Am Sociol Rev 81(5):949–980. https://doi.org/10.1177/0003122416663683

Chirwa DM, Chenwi LM (eds) (2016) The protection of economic, social and cultural rights in Africa: international, regional and national perspectives. Cambridge University Press, Cambridge, United Kingdom, New York, NY

Clough J (2014) A world of difference: the Budapest convention on cybercrime and the challenges of harmonisation. Monash UL Rev 40(3): 698

Colli A, Nicoletta C (2013) The role of the state in the third industrial revolution. In: Giovanni D, Louis G (eds) The third industrial revolution in global business. Cambridge University Press, Cambridge, pp 229–251. https://doi.org/10.1017/CBO9781139236706.008

Council of Europe (2004) Convention on cybercrime. No. 185. vol. ETS No. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

De Vattel E (2011) The law of nations: or, principles of the law of nature, applied to the conduct and affairs of nations and sovereigns. In: Chitty J (ed). Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9781139

Dekker IF, Werner (eds) (2004) Governance and international legal theory. Nova et Vetera Iuris Gentium Series A, Modern International Law 23. Nijhoff, Leiden

Dugard J, Plessis MD, Katz A, Pronto AN (eds) (2011) International law: a South African perspective, 4th edn. Juta, Cape Town

European Union (2016) Regulation (EU) 2016/679 of the European parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation), vol 2016/679

Fang B (2018) Cyberspace sovereignty: reflections on building a community of common future in cyberspace. Springer, Singapore Beijing

Freeman DH, de Jongste H (1984) A new critique of theoretical thought: the necessary presuppositions of philosophy (Dooyeweerd, H. Works. Ser. A, V. 1). Paideia Press Ltd

Gill TD, Robin G, Robert H, Tim M, Christophe P, Jessica D (eds) (2014) Yearbook of international humanitarian law vol 15, 2012. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-90-6704-924-5

Goldring J (1998) Globalisation, national sovereignty and the harmonisation of law. Unif Law Rev 3:435

Groscurth CR (2018) Future-ready leadership: strategies for the fourth industrial revolution. Praeger, Santa Barbara, California

Grotius H (1925) De Jure Belli Ac Pacis "On the Land of War and Peace." Carnegie ed. vol. chapter I

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, and UN Secretary-General (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/150. New York, NY. https://digitallibrary.un.org/record/799853?ln=en

Hathaway, OA, Rebecca C (2012) The law of cyber-attack. Digital Commons Yale Law, Faculty Scholarship Series, no. Paper 3852

Howlett M (2018) Policy analytical capacity: the supply and demand for policy analysis in government. In: Xun W, Michael H, Ramesh M (eds) Policy capacity and governance: assessing governmental competencies and capabilities in theory and practice. Springer International Publishing, Cham, pp 49–66. https://doi.org/10.1007/978-3-319-54675-9_3

Island of Palmas Case (or Miangas), United States v the Netherlands, Award, (1928) II RIAA 829. n.d

Iyi J-M (2016) Humanitarian intervention and the AU-ECOWAS intervention treaties under international law. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-23624-7

Janssen M, van den Hoven J (2015) Big and Open Linked Data (BOLD) in government: a challenge to transparency and privacy? Gov Inf Quart 32(4):363–368. https://doi.org/10.1016/j.giq.2015.11.007

Jayasuriya K (2001) Globalization, sovereignty, and the rule of law: from political to economic constitutionalism? Constellations 8(4):442–460. https://doi.org/10.1111/1467-8675.00252
Kelsen H (1961) General theory of law and state. Russell & Russell, New York
Kosseff J (2017) Defining cybersecurity law. Iowa Law Rev 103:985
Kriangsak K (2017) Public international law of cyberspace. Law, governance and technology series, vol 32. Springer, Cham
Kulesza J (2009) State responsibility for cyber-attacks on international peace and security. Polish Yearbook Int Law 29:139–151
Macak K (2016) Is the international law of cyber security in crisis? NATO CCD COE Publications 127, Tallinn, Estonia
Marwala T, Lagazio M (2011) Militarized conflict modeling using computational intelligence. Advanced information and knowledge processing. Springer London, London. https://doi.org/10.1007/978-0-85729-790-7
Michelman FI (1995) Always under law? Const Commentary 12:227
Mihr A (2016) Cyber justice: cyber governance through human rights and a rule of law in the internet. US-China Law Rev 13(4). https://doi.org/10.17265/1548-6605/2016.04.002
Pascariu C, Ionuţ-Daniel B, Ioan B (2017) Investigative analysis and technical overview of ransomware based attacks. Case Study: WannaCry. Int J Inf Secur Cybercrime 6(1): 57–62. https://doi.org/10.19107/IJISC.2017.01.06
SADC (2013) Harmonization of ICT policies in Sub-Saharan Africa—computer crime and cybercrime: South African development community model law
Schwab K (2016) The fourth industrial revolution. World Economic Forum, Cologny/Geneva
Sendler U (ed) (2018) The internet of things: industry 4.0 unleashed. Springer Vieweg, Berlin, Germany
Smith PAC, Pourdehnad J (2018) Organizational leadership for the fourth industrial revolution: emerging research and opportunities. Advances in Logistics, Operations, and Management Science (ALOMS) Book Series. IGI, Business Science Reference, Hershey PA, USA
Steyn L (2017) Data loss will make you wanna cry. The M&G Online. https://mg.co.za/article/2017-05-19-00-data-loss-will-make-you-wanna-cry/
Teitel R (2013) Author's response to Martti Koskenniemi's review of humanity's law. Ethics Int Affairs 27(02):233–234. https://doi.org/10.1017/S0892679413000154
The Lotus Case (France v. Turkey), PCIJ Reports, Series A, No. 10. 1927
United Nations (1979) Agreement governing the activities of states on the moon and other celestial bodies, vol 1363 U.N.T.S. 3
Venktess K (2017) Up to million computers hit in biggest cyber attack ever | Fin24. https://www.fin24.com/Tech/Cyber-Security/up-to-million-computers-hit-in-biggest-cyber-attack-ever-20170515
von Heinegg WH (2014) The Tallinn manual and international cyber security law. In: Terry DG, Robin G, Robert H, Tim M, Christophe P, Jessica D (eds) Yearbook of international humanitarian law, vol 15, 2012. T.M.C. Asser Press, The Hague, pp 3–18. https://doi.org/10.1007/978-90-6704-924-5_1
Vyas L (2018) Re-Invention of the Public Sector Training. In: Ali F (ed) Global encyclopedia of public administration, public policy, and governance. Springer International Publishing, Cham, pp 5411–5416. https://doi.org/10.1007/978-3-319-20928-9_2545
Weil P (1983) Towards relative normativity in international law? Am J Int Law 77(3):413. https://doi.org/10.2307/2201073
Weiler J (2001) The rule of lawyers and the ethos of diplomats : reflections on the internal and external legitimacy of WTO dispute settlement. Harvard Jean Monnet Working Paper 9. Harvard Law School, Cambridge, MA
World Economic Forum (2019) Leading through the fourth industrial revolution: putting people at the centre. World Economic Forum