APPLYING PRINCIPLES OF INTERNATIONAL LAW TO CYBER

excerpt from forthcoming study of
Cyber Arms Control

Edward M. Roche

April 2020

1 Questions for Reviewers

Instructions

This document is an excerpt from a larger paper on Cyber Arms Control.

If you have a few minutes as a reviewer, please answer these questions either in writing or via audio/video.

Email your response to dsi@cyberarmscontrol.org

Thank you!

1. Are there any factual errors in the analysis?
2. What are the most compelling arguments *against* using the United Nations Security Council for cyber peacekeeping?
3. Is the writing style clear, or is it fuzzy?
4. Is the writing exciting or is it boring and tedious?
5. What can be done to improve the concept?
6. How realistic is the idea? (Which stakeholders would oppose the idea and why? Which stakeholders would support the idea?)
7. What can be cut?

Contents

List of Tables

List of Figures

2 Enduring Problems in International Law

> *When we lengthen our gaze, we will see more clearly that law and strategy have always been mutually excited switches on the same circuit, and that the State itself . . . is the mechanism of feedback. . . . The international legal environment reflects the strategic environment, much as commercial law reflects the market, or the legislation of government reflects events in politics.*[1]

One of the enduring problems in applying international law to the world of cyber stems from its nature as a new technology. When the delegates forming the United Nations met in San Francisco, there were no computers. Having survived the horrors of the Second World War, they were concerned with preventing another military disaster. This is the traditional inclination of diplomacy after *every* great war, but in spite of best efforts, success never has been found, except temporarily.

> *Only the dead have seen the end of war.*[2]

The result of this mind-set shows up in the language of international law. Conflict between nation states always is described as "armed" conflict. Since there were no computers, the term "armed" refers primarily to guns and bombs—things that kill and maim. Aggression is described as "armed" attack.

For some unknown reason, cyber weapons even if deployed by a nation's military forces, never have been described as "arms". Generally, the term "armament" refers to a wide range of military equipment. Rifles, machine guns, battleships, stealth bombers, ICBM rockets carrying thermonuclear weapons, chemical sprays, electro-magnetic pulse transmitters, radio frequency jammers – are are considered part of the integrated arsenal of a nation's military. Cyber has become merely another weapon in this arsenal.

In spite of this, legal scholars have debated endlessly over whether or not a cyber attack is an "armed" attack. Are cyberweapons "arms"? Even a multi-million cyberweapon such as Stuxnet, which was prepared partially at the Oak Ridge National Laboratory, home of the first enriched uranium production for the world's first atomic bomb, and tested extensively in government and military funded laboratories, in the same way other weapons are, in the view of some is not an "armament".

This defies belief, and leads to very serious consequences in application of international law. For example, it is a fundamental principle in international law that a nation state has a right of self defense against an *armed* attack.

We can see this problem in the language adopted by the United Nations General Assembly in 1970 regarding principles of international law.[3] This

[1] Philip Bobbitt, The Shield of Achilles (New York: Alfred A. Knopf, 2002) p. 355

[2] General MacArthur's May, 1962 farewell address at West Point, and inscription on Imperial War Museum in London.

[3] Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, General Assembly Resolution 2625 (XXV) of the Twenty-fifth Session, 1883rd plenary meeting, adopted 24 October 1970

declaration proclaimed a number of principles of international law. It contains a number of verbs that describe what States are *not* supposed to do. In the Preamble, it specifies that States should not "intervene in the affairs of any other State". There is no description giving details of what "intervene" means in this context. States also should not use "coercion", which can be "military, political, economic or any other form". The prohibited object of coercion is either "territorial integrity" or "political independence" of the victim States.

It appears that the language in the Declaration is purposefully vague and open for interpretation. For example, when the Declaration says "or any other form of coercion" would it be unreasonable to include the category of "cyber coercion"?[(4)] After all, cyber coercion against the political independence of a State is remarkably similar to the concept known as information operations.

The Preamble also states that

> it is essential that all States shall refrain in their international relations from the threat or use of *force* against the territorial integrity or political independence of any State, or *in any other manner* inconsistent with the purposes of the United Nations.[(5)]

The language uses the term "force" instead of "armed forces" or "armed attack". This makes the terminology broader in its scope. The concept of "force" is more general. Is it reasonable to include "cyber force" under the umbrella of this concept? If the term "force" was limited to use of traditional (non-cyber) armaments, then it would fit with the object of "territorial integrity" because traditional weapons usually are associated with violent military occupation of captured territory. The use of the same type of weapons against the "political independence" of a State is more abstract. Territory is concrete, political independence is intangible. Consequently, it is reasonable to think of "force" meaning intangible types of force such as propaganda or information operations. Finally, the language "in any other manner inconsistent with the purposes of the United Nations" is the broadest concept of all. This is so broadly defined it seems unreasonable to associate it with *only* the use of conventional military weapons. For example, an economic boycott is a type of force that may be applied against one State by another, but it does not involve use of traditional military weapons. In consequence, it seems untoward to exclude use of *cyber force* by one State against another as being within the meaning of this language in the Preamble. This would mean, of course, that using a cyber weapon would be a violation of international law, assuming it is possible to define what is meant by the term "cyber weapon".

The Declaration states that

> Such a threat or use of force constitutes a violation of international law and the Charter of the United Nations and shall never be employed as a means of settling international issues.[(6)]

It also condemns use of "propaganda for wars of aggression".

[(4)] *Ibid*, para. 10
[(5)] *Ibid*, Preamble, para. 11, (emphasis added)
[(6)] *Ibid*

Another important international legal principle is "the duty not to intervene in matters within the domestic jurisdiction of any State". Here the term "arms" is used.

> Consequently, *armed* intervention and *all other forms of interference* or attempted threats against the *personality* of the State or against its *political, economic and cultural elements,* are in violation of international law.[7]

Again, the reference to the use of "arms" is broadened by the language "all other forms of interference". This would include cyber or information operations. We can see that the "soft" tools of information and cyber technology may be assumed to fit because they match the type of effect being sought. There is no reference to "territorial integrity", but instead to "political, economic and cultural elements". Apart from dropping bombs on movie production studies or dance theatres, which in any case would be illegal under the rules of war because they are not military targets, it is more appropriate to match information and cyber tools of force against these targets. For example, the term "political" refers to the agreed upon social contract controlling relations between citizens and their government. This is a completely abstract and theoretical thus intangible concept. It may not be shot or bombed. Cyber tools are a better match, and thus fit into this definition of international law.

Finally, the Declaration states that

> The principles of the Charter which are embodied in this Declaration constitute basic principles of international law.[8]

At the time the United Nations General Assembly made this Declaration, information technology was developing rapidly, but had not reached the general consumer. The first supercomputer, the Control Data CDC 6600, had been developed four year earlier, and the floppy disk was only 2-3 years old. Intel had been founded in the previous year.[9] The first scientific calculator had just been released by Hewlett-Packard, the model 9100A. ARPANET was started in the U.S. Department of Defense, later to evolve into the Internet. The Unix operating system was being developed. Later it evolved into the C source code, Linux, and MacOSX. The same month of this Declaration, the first dynamic RAM chip was introduced by Intel, with a capacity of 1024 bits. The world of social media and socially pervasive computing we see today[10] was completely unknown. No one was using the word "cyber". Not a single expert drafting this international law could possibly have expressed the concept of "cyber force", or "cyber war" or "cyber intervention in the internal affairs" of other States.

[7] *Ibid*, (emphasis added)

[8] *Ibid*

[9] We are counting back one year to 1969 to account for the negotiating time needed to develop the Declaration.

[10] Approximately 2019-2020

Purpose	Principle
General	*Clausula rebus sic stantibus*
	Pacta sunt servanda
Interpretation	*Ex aequo et bono*
	Estoppel
	Venire contra factum proprium
	Abus de droit
Fair Procedure	*Nemo iudex in sua causa*
	Audiatur et altera pars
	No arrest without trial
Substantive	*Contrat administratif*
	Unjust enrichment

Table 1: Principles of International Law and their Function

3 International Legal Principles for Cyber Discussed by the Group of Governmental Experts

In its 2015 report, the Group of Governmental Experts reviewed several principles of international law that are applicable to State use of ICT.[(11)] These principles were listed after the Group of Governmental Experts emphasized that any State, member of the United Nations, already is bound by the UN Charter.[(12)] The mention in the Group of Governmental Experts Report of these principles is without notable detail.

3.1 Principles of Necessity

The principle of necessity in international law asserts that a State may take actions that otherwise would not be legal providing it is used in self-defense. If this happens, then these extra-legal actions may be found to be constitutional. In particular, under *ius ad bellum*, States may take "illegal" actions if they are necessary for self-defense. This is considered to be a principle of customary international law.

3.2 Principle of Distinction

The principles of distinction in international law is a traditional rule that operates to make a distinction between civilians and combatants. In general, military force is to be used primarily against the military forces of the opponent. It is not to be used against "innocent" civilians.

This principle was observed somewhat up until the Second World War. There, the use of "strategic bombing" ensured that civilians were killed. In terms of bombing to death civilians, there were two types of activities:

[(11)] *See* pp. 12–17, §VI, para. 24–29, Report of the Group of Governmental Experts on Developments in the Field of Information an Telecommunications in the Context of International Security, UN Document A/70/174 (22 July 2015).

[(12)] This is discussed *infra* pp. **??**–**??**.

strategic civilian bombing, and non-strategic. The concept of "strategic" bombing is that bombs are dropped on targets that if damaged will inhibit the ability of the enemy army to conduct the war. Examples would be be bombing of railroad lines that are essential for transportation and logistics. Another example would be the bombing of telecommunications switching centers in order to degrade the command control operations of the enemy.

Any bombing or destruction of facilities that might help the military effort would come under this category. For example, during the Second World War, the German army had built on the small island of Peenemünde[13] an Army Research Center to develop the V-2 liquid-propellant rocket. The facility housed a large number of civilian engineers and others to work on the complex project. The facility was bombed on 18 August 1943 by the Royal Air Force of the United Kingdom. The USA bombed the facility on July 18th, August 4th and 25th. Although military persons were killed, so were engineers and civilians working in a support role.[14]

Later in the war, the city of Dresden[15] was bombed using high-explosive bombs and incendiary devices. This created a firestorm, destroyed more than 1,600 acres and killed around 25,000 persons, almost all civilians. This was not strategic bombing. The theory behind this type of bombing was that by attacking the civilian population, it would weaken the resolve of the German people to fight the war.[16] In the war with Japan, the United States used similar conventional bombing to destroy 67 Japanese cities, and on August 6th and 9th dropped nuclear weapons on Hiroshima and Nagasaki killing approximately 355,000 persons.

In spite of these unfortunate events of the Second World War, the principle of Distinction still exists. It remains doctrine that the primary target of military fighting is the *military* of the opposing side. In the cyberwar context, military objectives must be distinguished from civilian objectives.[17]

The only application of this principle for cyber operations is that it *sanctions* the use of cyber in connection with military force in a conflict. In any situation where military action might legitimately be taken, cyber operations are within international law. Consequently, cyber operations taken in preparation for kinetic military action, and in advance of such action also are valid under this interpretation of international law. There is no distinction regarding timing. Presumably, offensive cyber operations in support of a *future* kinetic military action are legitimate, even if they are indefinitely in

[13] Location 5408'0"N 1346'0"E

[14] Eventually the V-2 project was moved to underground factories located at Nordhausen. (5130'18"N 1047'28"E)

[15] 512'N 1344'E

[16] It did not accomplish this objective.

[17] *See* Michael J. Adams & Megan Reiss, "International Law and Cyberspace: Evolving Views", Lawfare, March 4, 2018 quoting Harold Koh, Legal Adviser, US Department of State. ("The *jus in bello* principle of distinction applies to computer network attacks undertaken in the context of an armed conflict. The principle of distinction applies to cyber activities that amount to an "attack"—as that term is understood in the law of war—in the context of an armed conflict. As in any form of armed conflict, the principle of distinction requires that the intended effect of the attack must be to harm a legitimate military target. We must distinguish military objectives — that is, objects that make an effective contribution to military action and whose destruction would offer a military advantage — from civilian objects, which under international law are generally protected from attack.")

advance.

The logical consequence of this is that offensive and purely cyber operations are valid, since the use of kinetic military force always is a possibility, or since they may be a minimal use of force to accomplish State objectives.

3.3 Principle of Humanity

A related concept of the principle of humanity in international law. This protects combatants from unnecessary suffering in the event of conflict. Its basic notions go back at least as far as Saint Augustine of Hippo.

> "To be legitimate a war had to be either defensive or fought to remedy some grave injustice perpetrated by the enemy; it had to be carried out under the command of a properly constituted public authority, not as private vengeance; and its *conduct had to be confined within some bounds of human decency*, to be waged without . . . violence, cruelty, savagery, lust for power, and the like."[18]

For example, if enemy soldiers are captured and put into detention until the end of the war, they are not supposed to be tortured or executed. They should be given generally "humaine" treatment. An early example of international humanitarian law is found in the preamble to the 1899 Hague Convention.

> [P]opulations . . . remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the *laws of humanity*, and the requirements of the public conscience.[19]

This was known as the "Martens Clause".[20] In its opinion on the legality of using nuclear weapons, the ICJ stated that:

> The cardinal principles contained in the texts constituting the fabric of humanitarian law are the following. . . . States must never make civilians the object of attack and must consequently never use weapons that are incapable of distinguishing between civilian and military targets.[21]

Humanitarian law is derived from the tradition of *mission civilisatrice*.[22] "The end result [of application of the principle of humanity] is a legal regime

[18] Lived 354–430. *See* James Henderson Burns (*Ed.*) The Cambridge History of Medieval Political Thought c. 350-c. 1450, Cambridge U. Press, 2008. Chapter *The Latin Fathers*, p. 115 (describing St. Augustine's view of the morality of warfare), (emphasis added)

[19] Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 29 July 1899. Preamble, para. 9, (emphasis added)

[20] Named after Fyodor Fyodorovich Martens, the Russian delegate to the Hague Peace Conference, *cited by* Advisory Opinion of 8 July 1996, Legality of the Threat or Use of Nuclear Weapons, 257 para. 78, International Court of Justice, 226-267 (1996)

[21] *Ibid*

[22] *See* the extensive review by Larissa Fast, *Unpacking the principle of humanity: Tensions and Implications*, 97 International Review of the Red Cross 115, 111-131 (2015)

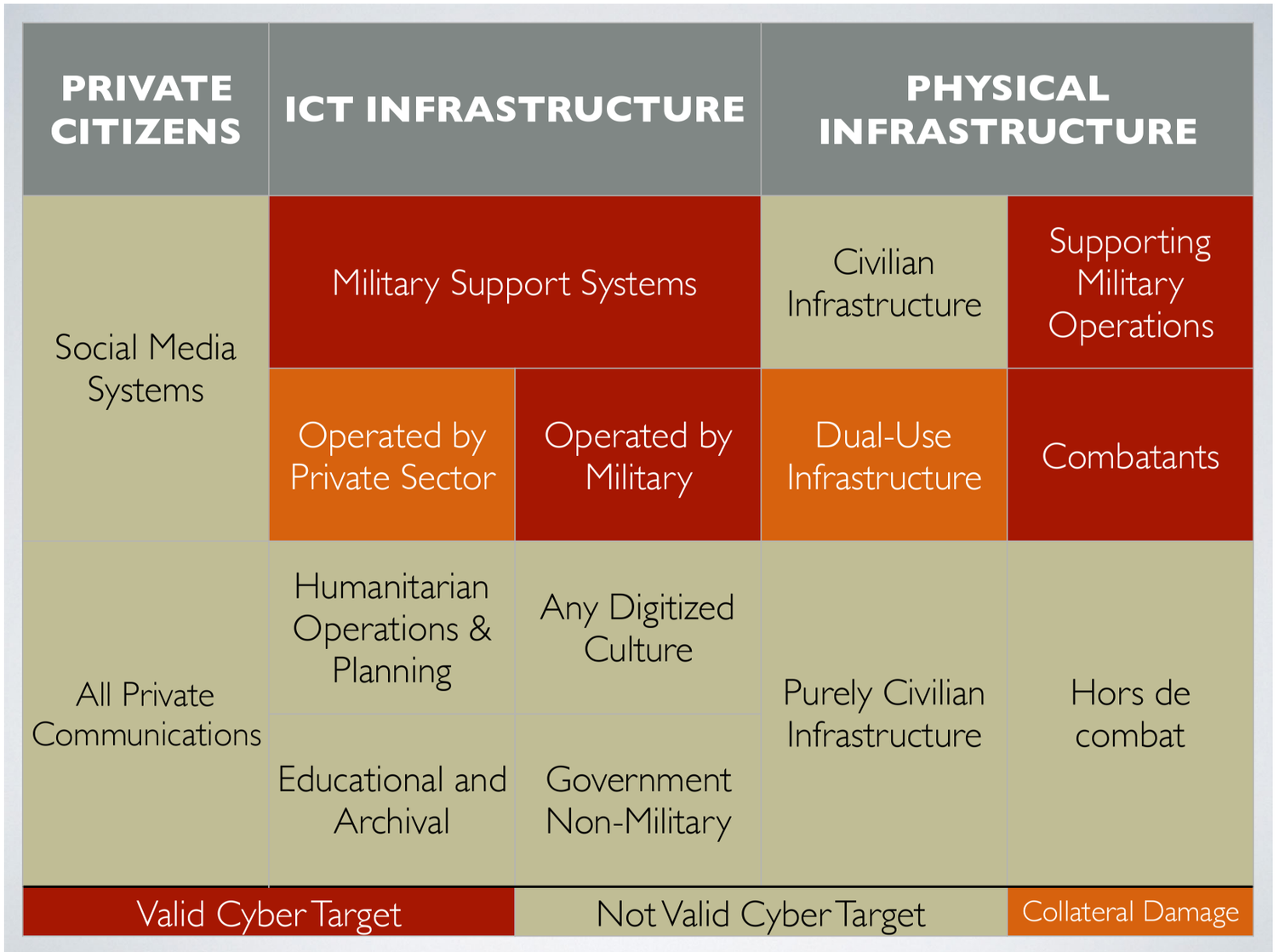

Figure 1: Cyber targeting and principles of international law.

that operates in favour of humanity rather than protecting the rights of States, and that restricts the excesses of State action."[23] Humanity is not a clearly defined legal norm. International humanitarian law, nevertheless, protects "civilians and other persons *hors de combat*."[24]

The application of international humanitarian law as *lex specialis* is a vector for development of binding norms.[25]

Applying notions of the principle of humanity to cyber operations during a conflict would require that civilians not involved in fighting would be protected, as would combatants who no longer were in the fight. It also would imply that nothing would be done to disrupt those cyber and informational processes that are set up to support humanitarian operations. Information operations supporting humanitarian impulses include ICT systems used for preparedness, needs assessment, analysis, joint planning and coordination, resource mobilization and allocation, including operationalization of private sector and public sector partnerships, implementation of models of delivery to aid the suffering and control systems informed by monitoring and evaluation applications.[26] Consequently, in a cyber emergency or conflict, this suggested norm would circumscribe the offensive cyber operations of any State, even against government targets, providing those ICT systems were involved in any aspect of humanitarian operations. This would in effect circumscribe any offensive cyber operations against civilian government agencies, leaving only military-related parts of the government, or other parties *directly* involved in supporting the military as cyber targets. Almost any data or supporting ICT system that supported any aspect of human health, food production and distribution, or education as well as both public and private non-military records are removed from the target list.

It would be impossible for any State to comply with this principle or norm of behavior unless it already had collected extensive cyber and technical intelligence mapping the cyber infrastructure of the target State. *One point of negotiation for a cyber arms control treaty would be the development of an identification protocol that would allow humanitarian ICT systems to be recognizable by incoming cyber weapons.* This would allow these systems to remain outside the boundary of a cyber attack.

3.4 Principle of Proportionality

The principle of proportionality in international law is derived from the theory of punishment. According to Yoram Dinstein, "The principle of proportionality is the key to the effective protection of civilians and civilian

[23] *Ibid* p. 117

[24] Kjetil Mujezinović Larsen and Camilla Guldanl Cooper, *Conclusions: Is there a 'principle of humanity' in international humanitarian law?*, in Kjetil Mujezinović Larsen, Camilla Guldahl Cooper, Gro Nystuen, *Eds.*, Searching for a 'Principle of Humanity' in International Humanitarian Law, Cambridge University Press, 2012, 355, 349–356

[25] *Ibid*p. 356

[26] *See* Figure 8, *Potential Impact of the Network Age on Humanitarian Action*, p. 33, UN Office for the Coordination of Humanitarian Affairs (OCHA), Humanitarianism In The Network Age 2013 (Emphasizing that "information [is] . . . a basic need in humanitarian response . . . information relevant to humanitarian action [should be] . . . shared freely. p. 7)

objects from the consequences of attacks in warfare."[27] The punishment should be proportional to the seriousness and harm of a crime. In fighting a conventional war, the shooting of a single shot should not be followed by the razing of an entire city in response. The principle is codified in the Protocol Additional to the Geneva Conventions:

> Among others, the following types of attacks are to be considered as indiscriminate: . . . (b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[28]

The principle is found also in Article 57 *Precautions in attack*:

> 1. In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.[29]

Of note in this codification is the reference to "civilian objects". According to customary international humanitarian law "Civilian objects are all objects that are not military objectives."[30] This definition is found in the Amended Protocol II on Conventional Weapons,[31] The concept of "military objective" is defined in paragraph 6.

> "Military objective" means, so far as objects are concerned, any object which by its nature, location, purpose or use makes an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

In application of these rules to a cyber emergency, it is clear that the principle of proportionality does not apply to targets that are connected to the military forces of the enemy. The primary purpose of this rule is to limit damage to non-combatants. The plain meaning of "object" is a physical thing, not an abstract arrangement of information. Following that logic, the

---

[27] Yoram Dinstein, *The principle of proportionality*, in Kjetil Mujezinović Larsen, Camilla Guldahl Cooper, Gro Nystuen, *Eds.*, Searching for a 'Principle of Humanity' in International Humanitarian Law, Cambridge University Press, 2012, pp. 72–84

[28] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977. *See* Article 51 *Protection of the civilian population.*

[29] *Ibid*

[30] *See* Rule 9: Definition of Civilian Objects, IHL Database of the International Committee of the Red Cross .

[31] Amended Protocol II to the Convention on Certain Conventional Weapons, Article 2(7), United Nations, *Treaty Series*, vol. 2048, p. 93; Doc. CCW/CONF.I/16 (Part I). ("Civilian objects" are all objects which are not military objectives as defined in paragraph 6 of this Article.") *see also* Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (with Protocols I, II and III) Geneva, 10 October 1980, United Nations, *Treaty Series*, vol. 1342, p. 137, Protocol III, Article 1(4) (containing the same language)

information systems and data of civilians would not be protected under the rule of proportionality.

Instead, "civilian objects" are defined in a negative way. They are anything that is not a "military objective". These are defined as "any object" that helps obtain military advantage. Computer and telecommunications systems are objects, as they are physical in nature. If the information or software operating a computer system is corrupted, leading to an immobilization of the computer, or even its destruction, and yet this is done using a non-kinetic attack, then it is no different from the immobilization of a power generator by putting sand into the fuel supply.

Destruction does not necessarily mean physical destruction, but for military purposes can imply merely that the functionality is eliminated. Consequently, the effect of the application to cyber emergency of the principle of proportionality is that any offensive cyber action under international humanitarian law should not do harm to any civilian information system or data, providing infliction of any harm would not assist in the attainment of military objectives. Like the use of conventional bombs to destroy the German city of Dresden,[(32)] cyber weapons should never be used in order to destroy civilian *information* infrastructure.

This is an important norm for the attainment of cyber stability. There is perhaps a hidden boost to the need for collection of cyber-intelligence. In order to meet these humanitarian objectives in a cyber emergency, it would be essential that previous research has identified the nature of the ICT infrastructure in the target State. It will be necessary to have identified civilian ICT in comparison to government or military ICT. Without this information, there is a risk of counter-military actions bleeding over into the civilian world.

An additional problem with application of the proportionality principle is that currently cyber war-fighting tools are being developed specifically to target national infrastructure. Should this happen, then there will be a significant effect on the civilian population. Under these norms suggested by the Group of Governmental Experts, the use of cyber for targeting civilian infrastructure is a violation of international law.

4 A Wider Landscape for International Law and Cyber

By 2016, some observers made the absurd assertion that the international system "can become as much an obstacle as a solution" in addressing jurisdiction issues that span national boundaries.

> Rooted in the treaties of the Peace of Westphalia . . . our international system, based on the territorial jurisdictions, the separation of sovereignties, and non-interference, struggles to handle the

[(32)] 5103'01" N 1344'14"E. 13th and 15th February 1945. British Royal Air Force (RAF) and United States Army Air Forces (USAAF) dropped more than 3,900 tons of high-explosive bombs and incendiary devices on the city center. Destroyed 6.5 square kilometers (1,600+ acres). 22,700–25,000 persons killed.

transborder digital realities of the twenty-first century.[33]

The original "inter-*national*" law involved the governance of relationships between nation States, centering to a great extent upon maintenance of diplomatic relationships, protection of diplomats[34] and the law of war. There are several sources of international law recognized in the Statute of the International Court of Justice (ICJ).[35] The jurisdiction of the Court is limited to disputes between nation States.[36] If the matter before the Court involves a public international organization, then the Court will accept information from these organizations "on their own initiative".[37] The Court will communicate back to the concerned international organization if any matter in a case before it pertains to the "construction of the constituent instrument" governing that organization. Presumably this may have an effect on future operations of that concerned international organization.[38]

In its consideration, the Court relies on several sources for international law, some specific, some more general and ill-defined. As it decides disputes (between nation States) submitted to it, the Court uses *four* sources of international law.[39] First, the Court examines any relevant international conventions so as to determine if there are any rules that are "recognized by the contesting states" that might be applied in making its decision. It may be the case, however, that in the same way that a civil contract may never cover applicable contingencies, the international convention may fall short of supplying specific language that may be used by the Court. In that case, the court may look to "international custom" which is "evidence of a *general practice* accepted as law".[40] This will work if there is in place enough of an international custom that can be identified. If for a long time, States have engaged in a certain behavior pertinent to the matter before the Court, then even though such behavior is not codified in an international convention, the Court may treat the customary behavior as a something *not* contrary to international law, and thus may expect it in relevant State behavior. In the absence of some type of customary behavior, and lacking any language in a relevant international convention, the Court may then look to "general principles of law recognized by civilized nations".[41] There is no definition for the meaning of "civilized nation". It is possible that this language is a relic from the 18th Century. The Statute of the Court does not specify the meaning of "general principles".

The Court may also refer to "judicial decisions and the teachings of the

---

[33] Betrand de La Chapelle and Paul Fehlinger, *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*, Paper Series, No. 28, Global Commission on Internet Governance, Chatham House, 2016, p. 13 Note: The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. One of its themes was "establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues". *Ibid*, p. iii, *See* `www.ourinternet.org`

[34] Diplomatic immunity

[35] *See* `https://www.icj-cij.org/en/statute`

[36] *See* Article 34: "Only states may be parties in cases before the Court."

[37] *Ibid*, Art. 34(2). This is similar to the *amicus curiae* ("friend of the court") path for interested parties to submit material to the U.S. Supreme Court.

[38] *See Ibid*, Art. 34(3)

[39] These are defined in Article 38

[40] *Ibid*, Article 38(1)(b)

[41] *Ibid*, Article 38(1)(c)

most highly qualified publicists . . . as subsidiary means for the determination of rules of law".[42]

If none of this works, then the Court is empowered to decide a case *ex aequo et bono*, providing it receives permission from the State involved to resolve the case in this manner.[43] Roughly this means that the Court takes all of the facts into consideration and then resolves the case in the most fair way it can ascertain. It does so because all of the other sources of international law are not there to rely upon.

"Information security" is a broader concept than "Cyber arms control". It is not well defined, and can include a large range of issues involving information technology, applications, telecommunications networks, mass media, information services, and the development of any social formation supported by these technologies. As a consequence, there is potentially a broader range of application for international law. General principles of international law also are not precisely defined. So if we attempt to apply these general principles of international law to a nebulous concept such as "information security", then a broad range of scenarios will present themselves.

The general principles of international law[44] are not precisely defined. Friedmann's view is that "general principles of law may be a necessary and inevitable way of filling a *lacuna*[45] in the interpretation of a specific [legal] question."[46] There are important fundamental principles in international law such as *clausula rebus sic stantibus* and *pacta sunt servanda*. Principles may be used for *a*) Defining an approach for interpretation of legal relationships between the parties involved in litigation; *b*) Establishing minimum standards of procedural fairness in any proceeding; and *c*) Identifying substantive principles of law that are sufficiently and widely and firmly recognized in the leading legal systems of the world as applied to international legal principles. See Table 1.

What are general principles? They appear to be ideas that underlie law, and appear in one form or another in more or less all judicial codes in the world, including capitalist, socialist, and Islamic systems.

4.1 *Ex aequo et bono* — Equity and Fairness in Information Disputes

If the Court is unable to use other sources of international law in making its decisions, then it may resort to general principles of equity. In traditional conceptions of equity, the balance of interests between the litigant parties is resolved by either compelling action of one or more parties, such as in the specific performance of a contract, or in the paying of monetary damages or compensation, even in the absence of a written contract under conditions where nevertheless a service has been performed.

---

[42] *Ibid*, Article 38(1)(d)

[43] *Ex aequo et bono* means roughly: *a*) *ex* "coming out of"; *b*) *aequo* "equality", "equal"; *c*) *et* "and"; *d*) *bono* "[the] good". or "according to the right and good" or "from equity and conscience".

[44] *Ibid*, Article 38(1)(c)

[45] *Lacuna*, "an unfilled space or interval; a gap." from Latin *lacus*, a lake.

[46] Wolfgang Friedmann, *The Uses of "General Principles" in the Development of International Law*, 57 Am. J. Int'l L. 280, 279–299, 1963

In the case of ICT or information services, principles of equity might be applied providing it were possible to place a monetary value on the provisioning of information, data or cloud processing services. It also is possible that if ICT related activities in one State were being performed but were having some type of untoward effect in a third country, then even in the absence of any type of international agreement or convention, principles of equity might be used to call for curtailment or other modification of that action within the originating State. This would possibly done under principles of equity.

4.2 *Estoppel* in Issues of Information Management and Security

Estoppel is a legal principle that prevents a party from having a claim recognized by a court.[47] In a contract, a promise made without consideration yet detrimentally and foreseeably relied upon is enforceable under the principle of *promissory estoppel*. Once an issue has been ruled on by a court, then the result of the judgment may not be subsequently challenged in another court under the principle of *res judicata*.

If a citizen relies on the improper interpretation of a law by a public official or other person in authority, then prosecutors may be estopped from bringing a suit against them under the principle of *entrapment by estoppel*. When parties are negotiating an agreement yet there is fraud, misunderstandings on facts, or other problems with inducement into the agreement, then one party may be estopped from enforcement of the agreement through the principle of *equitable estoppel*. The term "*deed estoppel*" is used to prevent raising issues regarding the legitimacy of signatures to an agreement if such signatures were made under a seal, such as being notarized.[48]

In the matter of use of ICT by States, this principle would require that any use of information or data that has an untoward effect within the jurisdiction of another State would need to be documented and noted, otherwise eventually the State suffering the consequences would be unable later to make an acceptable claim. In the case of the use of international development funds to provide ICT into another country, there is an underlying warranty of appropriateness and suitability for the ICT being supplied, and consequently should the supply chain for that ICT be purposefully and intentionally tampered with so as to provide eavesdropping capabilities to a foreign intelligence service, then principles of estoppel would tend to argue that the contract for providing the technology was null and void so there would be no need to pay for it, even if this promise of repayment had been part of the original agreement between the concerned states.

The same principles of *representation estoppel* would apply to the validity of an international agreement that allowed the providing of mass media information or cloud services into a State if it were discovered that the way in which these services were being provided were not in synchronization with the original representations made during negotiation of the agreement.

[47] The root of the word is Latin *stuppare* which means to stop up something, like placing caulk in a crack to prevent water from leaking through. A common related English word is "stopper", something that might be used to prevent the water from running out of a bath tub.

[48] There are several other types of estoppel.

The principle of *proprietary estoppel* would be applicable to information and data collected inside one State and yet moved outside of that State or otherwise used for purposes which within the originating State represent a type of property right in the data or information on the part of the parties from which it was compiled. Application of this same principle would possibly apply to collection of information by the government of one State if the information being collected concerned name-linked information regarding the citizens or enterprises found in another State.

4.3 *Pacta sunt servanda* for Information Operations and Security

The principle of *pacta sunt servanda*[49] is a fundamental principle of law. Once agreements are made, they are to be kept. If one of the parties does not fulfill their promises, then it is considered to be a breach of the agreement.

When agreements are made between States, each country is presumed to carry out its obligations, and consequently is deemed to be able to rely on the promises made therein by another State. If there is a conflict between the domestic law of a State and its obligations under the international agreement, then the principle of *pacta sunt servanda* compels that the international obligation will take precedent, and so domestic law usually may not be recognized as an excuse for failure to fulfill obligations made in an international agreement.

The practical implication of this general principle is that States should refrain from adhering to international agreements that are in conflict with their domestic law. One corollary of this principle may be that international practices, even if widely accepted, may not be controlling over the international activities of a State in the absence of a specific commitment of that State to these principles. In those cases, the "pact[a]" would not need to be "[ob]served".

In the realm of information security, there is a potential problem between obligations under international agreements and the internal policies or domestic laws of some nation States. In particular, some countries have enacted laws that place significant controls on the utilization of information within their sovereignty. Under the principles of *pacta sunt servanda*, these domestic laws and administrative regulations should not be the basis for failing to meet obligations contracted to in any international convention. For example, Article 55 of the United Nations Charter calls for the United Nations to promote "conditions of economic and social progress and development . . . and international cultural and educational cooperation; and . . . observance of, human rights and fundamental freedoms for all". In addition, Article 56 of the Charter places obligations on member States who by signing the Charter have "pledge[d] themselves to take . . . separate action . . . for the achievement of the purposes set forth in Article 55."[50]

However, defined, these "fundamental freedoms" universally are considered

[49] Latin: "agreements must be kept"

[50] Article 56 also provides an option for member States to take action [in support of Article 55] in cooperation with each other and the United Nations. So acting alone is not the only option.

to include the right of free expression and communication.[51]

In spite of this language, *every* member States has enacted laws that restrict in one way or another absolute freedom of speech and communication. For example, all States have laws that prohibit the leaking of classified or sensitive information considered to be a national secret. Laws of libel are another example of restrictions. The most frequently mentioned example is that there is no freedom to shout "fire" in a crowded theatre [as this would cause an unnecessary panic and result in persons being harmed.][52] This type of restriction on free speech in the United States has been interpreted broadly to make punishable the statements of a person during a riot when such language has the effect of incitement to crime.

In the age of social media, the same type of situation existed in Egypt during the "Arab Spring".[53] In that matter, social media and mass communications being carried over the Internet were blamed for civil war, insurgencies, violence, and overthrow of governments. It was after the Arab Spring that international dialogue picked up the thread of government intervention in social media and creation of a "kill switch" for the Internet. During the Arab Spring, some countries had taken action to block access to Twitter and Facebook.[54]

In August of 2019, India changed the status of Kashmir, and immediately thereafter cut off all telephone and data communications in the area.

The obvious connection between national security and happenings in social media increased activities by governments to engage in monitoring of communications, including use of extensive "deep packet inspection".[55]

---

[51] A discussion of Articles 55 & 56 is found in Alfred Verdross, Jus Dispositivum and Jus Cogens in International Law, 60 Am. J. Int'l. L. 59–60, 55–63 (1966) who writes "Among the purposes indicated there we find "universal respect for, and observance of, human rights and fundamental freedoms for all without distinction as to race, sex, language, or religion." quoting "The question of race conflict in South Africa resulting from the policies of *apartheid* of the Government of the Union of South Africa", General Assembly Resolution 616 B (VII) at the 401st plenary meeting, 5 December 1952 ("*Declares* that in a multi-racial society harmony and respect for human rights and freedoms and the peaceful development of a unified community are best assured when patterns of legislation and practice are directed towards ensuring equality before the law of all persons regardless of race, creed or colour, and when economic, social, cultural and political participation of all racial groups is on a basis of equality")

[52] As U.S. Supreme Court Justice Holmes wrote "[F]alsely shouting fire in a theatre and causing a panic is an example of an expression which in the circumstances were intended to result in a crime and were a clear and present danger [and could be punished]." Opinion of Justice Oliver Wendell Holmes, Jr. in *Schenck v. United States*, 249 U.S. 47 (1919)

[53] The Arab Spring took place in the early 2010s. It started in Tunisia, but primarily through social media and as amplified by mass media, the protests spread to Libya, Egypt, Yemen, Syria and Bahrain. In those countries, these communications produced an overthrow of the government, major protests and uprising with social violence and riots. Eventually some countries experienced civil war or insurgency movements.

[54] As well as to other types of social media.

[55] Deep packet inspection (DPI) is a process of intercepting communications and data flowing through the Internet and checking it for content. Depending on the content, the information may be blocked, or the originator [and recipient] of the communication can be flagged for investigation. When DPI is in place, *all* communications are being monitored by the government, generally without due process or probable cause.

4.4 *Clausula rebus sic stantibus* and Cyber Emergency

A concept closely related to *pacta sunt servanda* is *clausula rebus sic stantibus.*[56] It is an antidote to the obligations under *pacta sunt servanda.* It is an "escape clause".

It allows for a nation State to renege[57] on its obligations under an international treaty if there is a fundamental change of circumstances. There is no clear or specific listing of events that might constitute a "fundamental change of circumstancs".

The Vienna Convention on the Law of Treaties,[58] provides several ways that a nation State may escape its obligation under an international convention. Article 60[59] allows a state to renege on its obligations by either suspending its obligation or rejecting it altogether if the corresponding party has failed to perform. Article 61[60] allows a nation State to stop performing its obligations if it becomes impossible to do so because "the impossibility results from the permanent disappearance or destruction of an object indispensable for the execution of the treaty". Article 62[61] reflects the principle of *clausula rebus sic stantibus.* It allows a nation State to not perform its obligations if there is a "fundamental change of circumstances".

The Article contains few qualifications that must be met before failing to perform. First, the change in circumstances must not have been "foreseen by the parties".[62] Second, the change in *any* circumstance is not a justification for reneging. Instead, the circumstances that have changed must be an "essential basis of the consent of the parties" when they signed the agreement.[63] Third, the change in circumstances must be such that it will "radically . . . transform the extent of obligations still to be performed under the treaty."[64] Fourth, the change in circumstances may not involve a treaty that "establishes a boundary".[65] Finally, Article 62 is not used if the change in circumstances is caused by a breach of obligation by the nation State that now is claiming it no longer is bound because of the change. In other words, a nation State may not itself cause a change in circumstances, then use that change in circumstances as a reason to renege on its obligations; the change must originate somewhere else.[66]

The application of *clausula rebus sic stantibus* to information security necessarily would involve a change in circumstances that would justify a nation State in backing out of its obligations under an international convention that involves some aspect of ICT or information security, including international telecommunications and applications provisioning systems. For example, it is possible to envisage a cyber emergency caused by sabotage or even a

[56] *Clausula* "clause"; *rebus* "affairs", "matters"; *sic* "in this way"; *stantibus* "standing"
[57] From Latin *negare* to deny.
[58] Vienna Convention on the law of treaties (with annex). Concluded at Vienna on 23 May 1969, 1155, 1-18232 United Nations Treaty Series 198–512 (1980)
[59] *Ibid*, *Termination of Suspension of the Operation of a Treaty as a Consequence of Its Breach*, p. 346
[60] *Ibid*, *Supervening Impossibility of Performance*, p. 346
[61] *Ibid*, *Fundamental Change of Circumstances*, p. 347
[62] *Ibid*, 1
[63] *Ibid*, 1(a)
[64] *Ibid*, 1(b)
[65] *Ibid*, 2(a)
[66] *Ibid*, 2(b)

catastrophic systems failure not attributable to a malicious third party that would be of such consequence that a nation State would need to suspend its performance of international communications agreements, including allowing linkages and continuity of service with international record carriers.

To the extent that private international law is concerned, it is possible to draw a scenario in which a nation State cuts off cloud, applications, database, and social media services in response to either an internal social emergency, or so as to act in self-defense in response to aggressive *information based* behavior originating outside of its territory.[67] Finally, although this principle never has been invoked in response to a cyber attack, it is clear that such an attack originating outside the jurisdiction of a nation State possibly could cause so much disruption that *clausula rebus sic stantibus* would be applicable and open up many options for suspension of treaty obligations.

Clausula rebus sic stantibus could justify an Internet "kill switch".

4.5 *Nemo judex in causa sua* and Attribution for Cyber Conflict

The principle of *nemo judex in sua causa*[68] refers to the use of impartial triers of fact in determination of legal decisions. In the case of a nation State and international law, the principle means that if there is a conflict or dispute with another State, the determination of the outcome may not fairly be made by either State, but instead should be made by a different party. The presumption is that no party can be fair in its decision when its own interests are at stake.

In the case of a cyber emergency caused by an alleged attack originating in a different nation State, the implication of *nemo judex in sua causa* is that the State suffering the damage from the attack *may not* unilaterally assign attribution for the attack to another party. For example, in the 2016 presidential election in the United States, the U.S. government, through indictments and a variety of public statements, has placed blame on the *government* of Russia for the information operations that presumably interfered in the internal affairs of the United States. The Government of Russia has denied these allegations. If the principle of *nemo judex in sua causa* is applied, then the *attribution* for these cyber attacks (information operations) must be decided by parties *other than* either the United States or Russia.

Up to this point,[69] there is in place no international arrangement to resolve this type of issue. What would be the source of an international mechanism available to resolve this type of conflict? What court? Further thought might be given as to whether the International Court of Justice (ICJ) would have jurisdiction. The jurisdiction of the ICJ is provided for in

[67] In the case of private international law, it is likely that *a*) There has been language inserted into the contract agreement that provides an escape mechanism for State action in case of an emergency or potentially for any reason deemed to be in the national interest; or *b*) In the absence of such language, the nation State would be able to invoke the principle of national sovereignty and exclusive jurisdiction over all information based activities that occur within its national boundaries.

[68] *nemo* "no one"; [is to be the] *judex* "judge"; [of their] *sua* "own"; *causa* "cause", "lawsuit"

[69] Spring of 2020

Article 36.[70] In order for a cyber emergency attribution issue to be reviewed by the Court, it is merely required that the parties submit the matter.[71] *There does not appear to be any limitation on the type of case that may be submitted to the Court.* The Court also has jurisdiction over "all matters specially provided for in the Charter of the United Nations or in treaties and conventions in force".[72]

This would mean that if a cyber emergency was declared to be a "threat to international peace and security" through Article 39 of the United Nations Charter, then it possibly could be a matter of adjudication as to whether some particular nation State was the originator of the disturbance.

How would the Court go about its work? There are no rules of evidence or established practice in the ICJ for adjudication of an attribution problem in information security. However, under Article 38(d) the Court would be able to avail itself of the teachings of qualified jurists and *judicial decisions* of relevance to the case. In practical terms, this means that the ICJ already has at its disposal the considerable amount of case law and forensic methodology for cyber evidence that already has been developed and proven to be effective. For example, in a situation where *proxies* comprised of private individuals or organizations are operating on behalf of a nation State in conducting information operations, cyber terrorism, or launching cyber attacks against critical infrastructure, then the attribution tools already widely used could be employed to verify that the government of the accused Nation state was not *directly* responsible for the cyber emergency.

In other cases, a variety of cyber forensic techniques could be used to verify that the originating point for a cyber emergency is in a facility that is directly under the control of the accused nation State. Such a situation took place with the uncovering of Chinese cyber espionage operations,[73] but there are many other examples, and long history of cyber and computer crime cases in the United States, Europe and elsewhere upon which the ICJ could draw for its work under Article 38(d).

One catch for Article 36(1) is that both parties must submit the matter to the Court for its work. What happens if one nation State is the subject of attributory accusation, but then refused to submit to adjudication of the Court? Unless the accused nation State agreed to go to the Court, it would be impossible to come to any legal decision regarding attribution for a cyber attack or cyber emergency.

There could be many reasons for a nation State refusing to agree to jurisdiction. These include: *a*) It might refuse to allow jurisdiction because it is clear that in order to carry out an investigation in the nature of cyber

---

[70] *See* Statute of the International Court of Justice, Done at San Francisco, 24 October 1945, Article 36

[71] *Ibid*, Article 36(1) "The jurisdiction of the Court comprises all cases which the parties refer to it".

[72] *Ibid*

[73] *See* for example, Indictment, United States of America v. Wang Dong, et. al., Criminal No. 14-118, U.S. District Court, Western District of Pennsylvania, May 1, 2014. "Defendant SUN targeted one of the employees working in the relevant division of U.S. Steel with an e-mail message, known as a "spearphishing" message, that was designed to trick the employee who received it into allowing SUN access to the employee's computer. . . . Defendant WANG stole hostnames and descriptions for more than 1,700 servers" p. 6; *See* also Exhibit F which contains empirical forensic evidence.

forensics, it would be necessary for an international fact-finding team to obtain access to information systems or other information such as internal communications that otherwise are classified or constitute national secrets, the exposure of which would constitute a derogation in its national security; *b*) The nation State could be of the view that the amount of time needed for the Court to investigate and come to a decision would be so great than its decision would have no practical consequence for a resolution of the cyber emergency, no matter what the decision was regarding its attributive responsibility; *c*) The nation State may not allow the Court to have such jurisdiction because it knows that it was not responsible for the cyber emergency, but is of the view that such an investigation would both impair its national honor by casting upon it a cloud of suspicion while at the same time allowing the true source of the cyber emergency to escape from any investigation; *d*) The nation State may conclude that the entire effort to shift the attribution matter to the Court is merely a subterfuge on the part of an enemy State to divert attention away from its own actions; *e*) It may be of the opinion that the way in which the issue is being framed for the Court is biased against it in the sense that while placing it under a cloud of suspicion, at the same time the judicial action refuses to also consider the possible responsibility of other parties for either originating or participating in or merely exacerbating the cyber emergency; *f*) The nation State may be unwilling to submit to jurisdiction of the Court because the framing of the issue does not allow for any justification for its cyber actions if they are *taken in response to the aggressive cyber activities of another nation State*; or *g*) for a number of other reasons.

Under the Statute of the Court, the cyber emergency attribution problem would be an example of "the existence of [a] fact".[74] but the determination of such a fact by the Court is *not* sufficient to justify its jurisdiction. Instead, only certain "facts" are relevant for jurisdiction of the Court. The fact to be determined must be one that "if established, would constitute a breach of an international obligation".[75] In this connection, there are two examples among many that are obligations that may be relevant to a cyber emergency. First, it is an international obligation under the United Nations Charter for a nation State to refrain from any action that would trigger Article 39 because it constitutes a threat to international peace and security. Second, a much more general obligation is found in Article 56 which requires nation States to support United Nations activities under Article 55.[76]

4.6 *Audi alteram partem (audiatur et altera pars)* and Rules of Evidence in Attribution for a Cyber Attack

Audi alteram partem[77] is a principle in law that requires the trier of fact to hear out the arguments by all involved parties. So if one party is the plaintiff, then before rendering a judgment, in order to have substantial justice, the court must hear the countervailing arguments or justifications of their actions by the party that is on the defensive.

---

[74] *Ibid*, Article 36(c)
[75] *Ibid*
[76] *See* Page 17
[77] *audi* "[to] hear"; *alteram* "[the] other"; *partem* "part [of the case]"

The application of this legal principle is somewhat clear if it is a nation State that is being accused of being the source of a cyber emergency. In that case, *audi alteram partem* would require that the Court would provide an opportunity for the accused nation State to provide its counter-arguments to the accusation. The same would be the case if *both* nation States were blaming each other for originating the cyber emergency. For example, it might be necessary for the Court to determine which State had originated the cyber attack and which State was merely responding in a justified defensive way to the initial cyber aggression. This would be the case if both States were claiming that they were merely responding in a defensive way to the actions of the other.

A complication arises if one or more of the nation States is claiming that a different party *not* a nation State and *not* a party to the case was responsible for the cyber attack. For example, this would happen if a State claimed as its defense that a private company or individual was responsible for the attack. Here the problem becomes how to bring this non-State party into the Court for adjudication. This appears to be a problem with the jurisdiction of the Court, since it is designed to handle disputes between *countries*, and not handle matters regarding private corporations, or individuals. For the time being, there may be an emerging "norm" calling for nation States to avoid allowing private parties on its territory conduct offensive cyber operations targeting parties in different jurisdictions. In addition, States are obligated to refuse to allow their sovereign territory from being the base for cyber attacks that target other governments, individuals, or organizations outside of its territory. If this norm were to obtain the force of law or custom, then even though the accused government might claim that it was not responsible for the attack, then nevertheless it would be held responsible for the cyber attack merely because it was originating within territory within its sovereignty and jurisdiction. This would leave open the question of whether or not the private entity was working as a proxy for its government. This norm would short-circuit this problem because the government would be held internationally responsible, whether it was using the private organization as a proxy or not.

On the other hand, the nature of cyber warfare is such that it is possible to "spoof" Internet signals in a way that makes an attack originating from one location to have an appearance associated with attacks (or computer code) originating in a different location. In practical terms, this means that one government could launch a cyber attack against a different State, but disguise the code for the cyber attack to make it appear that the cyber attack was coming from a different place. Regardless of the situation, the general principle *audiatur et altera pars* implies that the Court would be required to entertain the defensive arguments of the accused side, even if that side were not a nation State. In this connection, as discussed before, the Court would be able to rely upon the cyber forensic evidence practices that already have been extensively developed in various tribunals.

4.7 *Unjust Enrichment* applied to Industrial Policies in Cyberspace

Unjust enrichment[78] is a legal concept that originates in contract law. Assume there are two parties to a contract. One party confers a benefit upon the other, but does not receive something ("proper restitution") for the benefit it gave. If this is a contract, the easiest example is that one takes delivery of a good then refuses to pay for it. Unjust enrichment is a simple, but universal principle of law. In the *Lena Goldfields Arbitration* the Court concluded that the government of the Soviet Union had taken the benefits from the investment in the gold mining operation, but had made it impossible for the corporation to make back its money, because the government had breached its contract and taken over the business.

> The Lena Goldfields Arbitration has ended in an award of nearly 13,000,000 [English pounds] in favour of the Company against the Soviet Government. . . . The concessions to the Company were made in 1925 . . . The Company would have had at its disposal 30 per cent, of the production of gold; half of the production of lead, copper and zinc; and 80 per cent, of the production of silver. . . . The Company had been promised originally that it should be free to trade as it liked . . . the Soviet fixed its own prices. Anyone who tried to buy privately from the Company was threatened with death. Much of the property of the Company was stolen, and the Company could get no redress. In the end members of the Company's staff were arrested and tried on the charge of being revolutionaries.[79]

Some writers make a distinction between *damnum emergens* (compensation for losses suffered) and *lucrum cessans* the amount of damages that need to be paid for loss of anticipated profits.[80]

The problem of unjust enrichment applied to international disputes regarding ICT would arise if government action within the jurisdiction of its own sovereignty took actions that appropriated the intellectual property of an information service, software, or hardware provider. This appropriation would need to take place under conditions in which the foreign ICT enterprise had been brought into the national market under different circumstances, and consequently faced a dramatic change in domestic policy.

Appropriation of intellectual property is similar to nationalization of mining assets, or otherwise government action having the effect of destroying the operational autonomy of the foreign enterprise. For example, in the Google matter involving China, on the pretext of national security or industrial policy, attempts were made aimed at seizing control of the search algorithms that were trade secrets.[81]

---

[78] [Fr.] *"Enrichissement sans cause"*

[79] *The Lena Goldfields Arbitration*, The Spectator 6 Sep. 1930, p. 2; *discussed in* Christoph H. Schreuer, "Unjustified Enrichment in International law", 22 Am. J. Comp. L. 288, 281–301, 1974; *also see* Wolfgang Friedmann, The Uses of "General Principles" in the Development of International Law, 57 *Am. J. Int'l L.* 296–7, 279–299 1963

[80] *See* Friedmann, p. 292–3

[81] A very large part of the value of Google derives from non-patented trade secrets.

> "China . . . modifies the conditions of competition in favor of domestic suppliers through its uneven enforcement of facially neutral laws."[82]

A problem might arise if a nation State curtails the business activities of foreign ICT corporations within its territory for purposes that are incompatible with its international treaty obligations relating to freedom of communications or other commitments that have the nature of being reliant on information. For example, if a foreign vendor of anti-virus or other computer security technology were licensed to operate within a nation State, but because of the emergence of a cyber emergency the government took steps to seize its technology or otherwise interfere with its business operations.[83] Under the principle of unjust enrichment, then the ICT enterprise should be entitled to compensation on a pattern similar to the *Lena Goldfields Arbitration*.

4.8 *Protection of Acquired Rights* and National Cyber Autonomy

Protection of acquired rights long has been recognized in international law.

> "[T]he principle of respect for vested rights . . . forms part of generally accepted international law . . . "[84]

Even though this principle was stated in 1930, it still still plays an important part in international controversies, including Brexit.[85] According to Lalive,

> "*expropriation* for a public purpose . . . is *permitted* by general international law under certain conditions as an exception to the general principle of respect for alien property."[86]

He specifies three types of acquired rights *a*) Property; *b*) Contractual rights; and *c*) Concessions,[87] yet he disagrees with Friedmann on whether or not acquired rights are a general principle of law. In his conclusions he writes:

> "The principle of respect for the acquired rights of aliens is not a general principle of law recognized by civilized nations, within the meaning of Article 38 of the Statute of the International Court of Justice. It is a part of customary international law? The answer is yes and no."[88]

---

[82] *See* Cynthia Liu, Internet Censorship as a Trade Barrier: A Look at the WTO consistency of the Great Firewall in wake of the Google-China dispute, 42 Georgetown J. Int'l L. 1128, 1199–1240 (2011); *see also* James A. Brander, Victor Cui, Ilan Vertinsky, China and intellectual property rights: A challenge to the rule of law, 48 J. of Int'l Bus. Stud. 908–921 (2017)

[83] The government might claim a change in conditions exempted it from its obligations. *See* discussion regarding *rebus sic stantibus* on Page 19.

[84] Permanent Court of International Justice, Series A, No. 7, p. 42 *Certain German Interests in Polish Upper Silesia*, quoted by Pierre A. Lalive, The Doctrine of Acquired Rights, in Rights and duties of private investors abroad (Symposium on the Rights and Duties of Foreigners in the Conduct of Industrial and Commercial Operations Abroad.) 145, 165 Albany: M. Bender (1965).

[85] *See* Michael Waibel, Brexit and Acquired Rights, 111 Am. J. Int'l L. 440-44 (2017)

[86] Lalive, p. 164

[87] *Ibid*, pp. 183-5

[88] *Ibid*, p. 200

The issue of protection of acquired rights generally is connected closely with the problem of unjust enrichment (Page 24) and what happens when a State seizes the property of a alien.

In provisioning of cloud, information, and social media services, states can nationalize these foreign-owned businesses in the same way they can in other economic sectors. It remains an intriguing question as to what is actually capable of being nationalized, given that applications and the business process logic they enable with information services may reside in another jurisdiction, different from where the data is kept.

The use of in-country data processing requirements long has been recognized as a non-tariff barrier (NTB) to trade in services.[89] Nevertheless, restrictions on export of name-linked personally identifiable information have been justified on privacy grounds. It is difficult to argue that this type of control over utilization of name-linked data is an expropriation, since the data may not be owned in the first place. The seizing of software code, trade secrets, and other knowledge in processing the data would, however, be an example of seizing property. As such, this principle would argue against the right to do this.

4.9 *Venire contra factum proprium* and Cyber Privacy or Autonomy

The principle of *venire contra factum proprium*[90] makes it a violation of law to show behavior that is inconsistent with past acts. It refers to the behavior of an entity, here a nation State, that in the past has been predictable and was relied upon, but suddenly and without warning changes behavior to the detriment of some other party. This also is known as *l'interdiction de se contredire au détriment d'autrui* (The prohibition [against] contradicting [oneself] [in a way that is a] detriment to others.)

When States[91] behave predictably in a certain way, and other parties over time come to rely upon that behavior, then if there is suddenly arbitrary inconsistent behavior and it causes harm to the the other party who has acted in reasonable reliance, then any rights that otherwise might be available to the State changing its behavior might be lost, suspended or modified. This principle is a form of good faith and fair dealing. "Reasonable reliance" by the harmed party means that there must be some justification for its reliance on the other party's conduct.

In the cyber world, sudden changes in cyber policies by States, even though implemented within their national sovereignty, might be subject to this principle if there were significant untoward effects felt elsewhere.

---

[89] Edward M. Roche, The Computer Communications Lobby, the U.S. Department of State Working Group on Transborder Data Flows and Adoption of the OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, Ph.D. Thesis, Columbia University in the City of New York, 1988

[90] *venire* "come"; *contra* "against", "not in accord with", "not in the same way as"; *factum* "how characterized"; *proprium* "self"

[91] or any party