

RETHINKING THE PROHIBITION ON
THE USE OF FORCE IN THE LIGHT
OF ECONOMIC CYBER WARFARE:
TOWARDS A BROADER SCOPE OF
ARTICLE 2(4) OF THE UN
CHARTER
IDO KILOVATY*

ABSTRACT

Cyber-attacks that cause physical consequences are considered to be in violation of the use of force prohibition should the effects reach a certain severity threshold. That premise does not extend to cyber-attacks that cause economic harm due to a dated distinction between kinetic and other effects.

This article presents the argument that Article 2(4) of the UN Charter on the prohibition on the threat or use of force ought to apply to economic cyber-attacks. As a result, the right of self-defense could be triggered by the gravest of economic cyber-attacks, as well as the UN Security Council authority under Chapter VII in response to an economic cyber-attack. The underlying assumption is that the effects

*Doctor of Juridical Science (S.J.D.) candidate at Georgetown University Law Center and a Cyber Researcher at the Minerva Center for the Rule of Law under Extreme Conditions, University of Haifa, Faculty of Law, Israel. I wish to thank Prof. Rosa Brooks, Prof. Alexa Freeman, Prof. Eric Jensen and Mr. Ido Rosenzweig for their valuable comments and suggestions for this paper.

of economic cyber-attacks can be just as severe and threatening as the effects of kinetic cyber-attacks, and therefore, there is a need to reformulate the boundaries of the use of force paradigm to encompass the additional range of harmful cyber activities. This article proposes a framework consisting of a set of factors to assess economic cyber-attacks under the use of force paradigm.

On April 23, 2013, a hacker group working with support of the Syrian regime calling itself the “Syrian Electronic Army” hacked the Twitter account of the Associated Press (AP). The hacker group posted the following tweet on the AP account: “Breaking: Two Explosions in the White House and Barack Obama is injured.”¹ That in itself would most likely not constitute an act of war. However, immediately after the fake tweet was posted, and in a matter of only two minutes, the Dow Jones index plunged by about one hundred forty-five points, which equates to nearly one hundred fifty billion dollars.² After it became clear that the tweet was fake, the market quickly recovered.³ This scenario

¹ Grace Wyler, *AP Twitter Hacked, Claims Barack Obama Injured in White House Explosions*, Business Insider (Apr. 23, 2013), <http://www.businessinsider.com/ap-hacked-obama-injured-white-house-explosions-2013-4>.

² Peter Foster, *'Bogus' AP Tweet About Explosion at the White House Wipes Billions off US Markets*, The Telegraph (Apr. 23, 2013), www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.

³ Patti Domm, *False Rumors of Explosion at White House Causes Stocks to Briefly Plunge; AP Confirms Its Twitter Feed*

demonstrates the dangerous potential of a single ‘hack’ to inflict tangible, quantifiable and substantial harm, on a statewide level. Much has been already explored with regard to cyber warfare.⁴ Mainly, the current use of force scholarship focuses on cyber-attacks that cause direct or indirect physical consequences, also known as ‘kinetic cyber-attacks’ (KCA).⁵ KCAs concern the international community for many reasons. Mainly because KCAs are capable of bringing destructive physical outcomes, which were previously reserved to the domain of military kinetic weaponry. However, the concern does not stop there. Unlike military kinetic weapons, the production of malicious cyber tools (such as viruses⁶

Was Hacked, CNBC (Apr. 23, 2013), www.cnbc.com/id/100646197#.

⁴ See e.g., HEATHER DINNISS, CYBER WARFARE AND THE LAWS OF WAR (2014); MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW (2014).

⁵ See Scott Applegate, *The Dawn of Kinetic Cyber*, 5th International Conference on Cyber Conflict (2013), in which the author defines ‘kinetic cyber’ as “cyber attacks that can cause direct or indirect physical damage, injury or death solely through the exploitation of vulnerable information systems and processes”, available at: https://ccdcoe.org/cycon/2013/proceedings/d2r1s4_applegate.pdf.

⁶ See *The Tech Terms Computer Dictionary, Malware*, TECHTERMS.COM, <http://www.techterms.com/definition/malware>, “Like a biological virus, a computer virus is something you don’t want to get. Computer viruses are small programs or scripts that can negatively affect the health of your computer. These malicious little programs can create files, move files, erase files, consume your computer’s memory, and cause your computer not to function correctly. Some viruses can duplicate themselves, attach themselves to programs, and travel across networks. In

and worms⁷) and the employment of disruptive cyber techniques (such as DDoS⁸) are relatively inexpensive, quick and they do not require prolonged training.⁹ Moreover, the state does not have the exclusivity over the possession of those cyber tools and techniques, but virtually any individual or group can acquire the necessary skills training and equipment to carry out harmful cyber-attacks.¹⁰

fact opening an infected e-mail attachment is the most common way to get a virus”.

⁷ *Ibid*, “Just like regular worms tunnel through dirt and soil, computer worms tunnel through your computer's memory and hard drive. A computer worm is a type of virus that replicates itself, but does not alter any files on your machine. However, worms can still cause havoc by multiplying so many times that they take up all your computer's available memory or hard disk space. If a worm consumes your memory, your computer will run very slowly and possibly even crash. If the worm affects your hard disk space, your computer will take a long time to access files and you will not be able to save or create new files until the worm has been eradicated... Unlike viruses and Trojan horses, worms can replicate themselves and travel between systems without any action from the user”.

⁸ *Ibid*, “A distributed denial of service [DDoS] attack tells all coordinated systems to send a stream of requests to a specific server at the same time. These requests may be a simple ping or a more complex series of packets. If the server cannot respond to the large number of simultaneous requests, incoming requests will eventually become queued. This backlog of requests may result in a slow response time or a no response at all. When the server is unable to respond to legitimate requests, the denial of service attack has succeeded”

⁹ See Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 JOURNAL OF THE NATIONAL ASSOCIATION OF ADMINISTRATIVE LAW JUDICIARY 602, 618 (2011); also, see Michael Schmitt, *The Law of Cyber Warfare: Quo Vadis?* 25 STANFORD LAW & POLICY REVIEW 269, 286 (2014).

¹⁰ See Jonathan Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on*

There is a consensus among the majority of western states as well as scholars on what international law norms are applicable to KCAs, *inter alia*, the use of force paradigm, international humanitarian law, international human rights law and more.¹¹ However, ECAs pose a greater challenge to international law. While KCAs can qualify as a use of force, ECAs are generally not considered ‘use of force’, because it is generally believed that economic force or aggression is not ‘force’ for the purposes of the prohibition on the use of force.¹² The reason for that lies within the drafting history and the context of Article 2(4) of the UN Charter, as well as the customary international law that supports this article.¹³

This article generally agrees with the notion that at this time economic force would not be considered a use of force, but it will also advance the argument that the jurisprudence of Article 2(4)

Tomorrow's Battlefield, DUKE LAW & TECHNOLOGY REVIEW p. 6 (2010).

¹¹ As indicated by the *Tallinn Manual on the International Law Applicable to Cyber Warfare* is an initiative of NATO's – Cooperative Cyber Defense Centre of Excellence, based in Tallinn, Estonia. The *Tallinn Manual* was published in 2012, and it is a non-binding formulation of the international law norms applicable to cyber warfare, which were unanimously agreed upon by the group of experts assigned to draft the *Tallinn Manual*. MICHAEL SCHMITT (ED.), TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (2013).

¹² Matthew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 449 (2011)

¹³ See Marco Benatar, *The Use of Cyber Force: Need for Legal Justification?*, 1 GOETTINGEN JOURNAL OF INTERNATIONAL LAW 375, 380-386 (2009).

should progress to adjust itself to the new reality of economic cyber warfare. By doing so, this article will provide a framework to assist victim states in the assessment process of an ECA. The article will conclude by positing that international law applicable to economic cyber-attacks is incomplete and requires more attention in order to avoid abuse by potential perpetrators in the future. The conclusion of the article will be that in order to effectively deter and hold perpetrators accountable, and until more comprehensive and specific treaty law is available, the most grave and severe economic cyber-attacks must be considered uses of force, which are prohibited by Article 2(4) of the UN Charter.

I. INTRODUCTION TO ECONOMIC COERCION & FORCE IN INTERNATIONAL RELATIONS

Economic cyber-attacks tease out the loopholes and shortcomings of the use of force paradigm, but in fact, economic force predates cyber-attacks by many years. In 1973, the Organization of Arab Petroleum Exporting Countries (OAPEC) decided to limit production and reduce export of crude oil to countries who supported Israel,¹⁴ with the goal of forcing Israel to withdraw from the occupied territories of the 1967 war, as well as to restore the rights of Palestinians.¹⁵

¹⁴ James Boorman, *Economic Coercion in International Law: The Arab Oil Weapon and the Ensuing Juridical Issues*, at ECONOMIC COERCION AND THE NEW INTERNATIONAL ECONOMIC ORDER 255 (RICHARD LILLICH ED., 1976).

¹⁵ *Ibid*, 257.

This embargo, which also gained the name “the Arab Oil weapon”,¹⁶ caused a worldwide shortage of oil, which in turn led to an increase of the price of oil almost by four times.¹⁷ The Embargo had a tremendous effect on the United States, as it realized that it was vulnerable and that a small group of states could dictate its foreign policy.¹⁸

The economic effects of the Arab Oil embargo were quite unprecedented, given that oil is a scarce resource essential for the day-to-day lives of mankind. The Embargo sparked the curiosity of many international law scholars, who had to grapple with the question of the legality of the Arab Oil embargo.¹⁹ Ultimately, different researchers reached various, and at times contradicting, conclusions on

¹⁶ Ibid, 255.

¹⁷ Roy Licklider, *The Power of Oil: The Arab Oil Weapon and the Netherlands, the United Kingdom, Canada, Japan, and the United States*, 32(2) INTERNATIONAL LAW QUARTERLY 205, 206 (1988).

¹⁸ On August 2, 1977, Henry Kissinger addressed the National Conference of State Legislators and said: “For the first time in our history, a small group of nations controlling a scarce resource could over time be tempted to pressure us into foreign policy decisions not dictated by our national interest”. Available at: http://www.larouchepub.com/eiw/public/1977/eirv04n32-19770809/eirv04n32-19770809_019-rockefeller_launches_campaign_to.pdf.

¹⁹ See Ibrahim Shihata, *Destination Embargo of Arab Oil: Its Legality Under International Law* 68(4) THE AMERICAN JOURNAL OF INTERNATIONAL LAW 591 (1974); Jordan Paust et al., *The Arab Oil Weapon - A Threat to International Peace*, 68 THE AMERICAN JOURNAL OF INTERNATIONAL LAW 410 (1974); Harmut Brosche, *Arab Oil Embargo and United States Pressure against Chile: Economic and Political Coercion and the Charter of the United Nations*, 7 CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW 3 (1974).

whether the Arab Oil embargo of 1973 violated international law.²⁰

The Arab Oil embargo demonstrates that a state (or a group of states) may cause widespread economic harm and impose certain policy choices on the coerced state. The Arab Oil embargo triggered widespread writing as to the characterization of the use of economic force under international law. However, States are still limited by the potential economic harm they can cause, depending on their resources and relative position in the international community. Thus, the economic harm that one State could cause to the other by limiting its trade was inherently limited by various factors, an assumption that differs from the main concept of causing economic harm through non-trade related means, such as ECAs.

²⁰ Compare Ibrahim Shihata, *Destination Embargo of Arab Oil: Its Legality Under International Law*, 68 Am. J. Int'l L. 591, 625-627 (1974) – “The oil measures taken by the Arab states were the result of the exercise of their "sovereign right" to dispose of their natural resources in the manner which best suits their legitimate interests. In exercising that right, the Arab states have not violated any established rule of international custom or any prior treaty commitment”, and; Paust, Blaustein, *The Arab Oil Weapon – A Threat to International Peace*, 68 Am. J. Int'l L. 410, 439 (1974) – “The impact of the use of this form of economic coercion has been substantial in terms of the persons affected and the goals impaired. It was a coercion that threatened and might still impair not only the general wealth, well-being, and power of numerous nation-states and peoples, but also, more specifically, their national defense and security. Thus, the coercion was of such mounting intensity and efficacy that it can be authoritatively proscribed as a violation of basic Charter goals and of Article 2(4)”

The states that can actually cause significant and widespread economic harm due to their exercise of economic force is limited, because only those states that trade a scarce resource or commodity, which has no other readily available alternative, can potentially harm the states subjects to the economic force. In today's world, it is difficult to point out to more than a few examples of such resources or commodities.

Economic force is not to be confused with economic coercion. Economic coercion is "efforts to project influence across frontiers by denying or conditioning access to a country's resources, raw materials, semi- or finished products, capital, technology, services or consumers".²¹ In other words, an economically superior state exerts its economic power over another state to affect certain political choices of the latter state. Economic force, however, is the effort of one actor to disrupt or harm the economic activities of a state, for the sole purpose of injury to that state.²² In that context, injury means

²¹ Tom Farer, *Political and Economic Coercion in Contemporary International Law*, 79 AMERICAN JOURNAL OF INTERNATIONAL LAW 405, 408 (1985).

²² Ibid, p. 411, Farer provides that "In order to be a violation [of aggression], the economic measures must, to begin with, have as their exclusive purpose causing injury to another state. Secondly, even in the unlikely case where the infliction of injury is its own and only reward, the coercion is excused if it is an act of self- defense or if it is a reprisal". Farer also quotes A. THOMAS AND A. J. THOMAS, JR., THE CONCEPT OF AGGRESSION IN INTERNATIONAL LAW 90-91 (1972) in which it is contended that economic coercion cannot be used "for the sole purpose of causing injury to and forcing the will of another state, unless [it] is used in the exercise of the right of self-defense or reprisal.". Although the matter here is *coercion* rather than *force*, the notion remains similar - an economic force used for the sole purpose of injury (in contrast to

the materialization of physical damages that amount to a national security threat, such as major disruption of day-to-day activities of the population, deaths, injuries and destruction.

ECAs bring back the discussion on the legality of economic force. However, this time the discussion is even more complicated, because ECAs can cause tremendous economic harm to victim states, and the perpetrators are not necessarily coercing the victim states, but rather exercising power for purposes of revenge, hatred, reprisal or just to escalate or support existing armed conflicts. The attackers are also not necessarily developed states who have economic power or scarce resources, but rather they can be underdeveloped states who decided to invest in a 'cyber army' due to their relative inexpensiveness and ease of use.²³

ECAs might represent a turning point in the way international law is practiced and interpreted. Although it was believed that 'the political debate [over economic force as use of force] on this point has lost most of its steam by now...'²⁴ it seems that ECAs sparks this debate once more, and requires immediate attention.

coercion) to the state would constitute a violation of the prohibition of the use of force.

²³ Even a state as isolated as North Korea invests in its own 'cyber army'. "South Korea has claimed that North Korea has a 6,000-member cyber-army dedicated to disrupting its military and government", See Associated Press in South Korea, "*North Korea Has 6,000-strong Cyber-Army, Says South*", THE GUARDIAN (Jan. 6, 2015), <http://www.theguardian.com/world/2015/jan/06/north-korea-6000-strong-cyber-army-south-korea>.

²⁴ BRUNO SIMMA (ED.), THE CHARTER OF THE UNITED NATIONS: A COMMENTARY, p. 209 (2nd ed., 2002).

II. ECONOMIC CYBER-ATTACKS: AN EXTENSION OF KINETIC CYBER-ATTACKS.

A tendency in the efforts to characterize and regulate different aspects of cyber warfare is to create different boxes for different types of actions within cyberspace. ECAs are no exception in that regard, the opposite is true. If we consider certain activities within cyberspace so harmful to various protected values that they trigger the right to a military response, there needs to be a clear and unambiguous definition of what those activities are. For some States ambiguity and lack of transparency are actually preferable since they allow some freedom of action that does not entail accountability. However, such actions could pose a threat to international peace and security which will need to be addressed by proper regulation.²⁵ Naturally, such dichotomous distinction is complicated and at times impossible to achieve, given the complexity of global politics and warfare in particular.

A preliminary question before fully analyzing ECAs is what KCAs are? As noted earlier, KCAs receive tremendous attention and thought, while ECAs remain unaddressed and often neglected or easily dismissed. Although this article deals with the threat that ECAs pose, it has to be acknowledged that KCAs and cyber warfare in general, provide the context that helps to understand ECAs as well.

A. KINETIC CYBER-ATTACKS (KCAS)

²⁵ See e.g. discussion on cyber espionage and how it threatens international peace and security without being explicitly illegal under international law at *Russell Buchan, Cyber Espionage and International Law* in RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE (2015).

KCAs are those cyber-attacks that are capable of causing physical effects, which are comparable to those effects caused by kinetic, traditional weapons.²⁶ The reason why cyber warfare researchers focus on the kinetic aspect of cyber-attacks is understandable. Since cyber warfare represents a new method of conducting offensive or defensive operations, the most obvious way to address it is not to show how it differs from traditional warfare, but rather how it is identical to it. Given that the effects caused by KCAs are pretty much the same as what we already experience, for example, death, injury and physical destruction of objects,²⁷ it is not too difficult, and even quite plausible, to argue that all our traditional rules and principles are applicable to this phenomenon regardless of its novelty.²⁸

²⁶ See William Banks, *The Role of Counterterrorism Law in Shaping ad Bellum Norms for Cyber Warfare*, 89 INTERNATIONAL LAW STUDIES 157, 169 (2013)

²⁷ Those tend to be popular indications of “kineticity”, See Michael Schmitt, *“Attack” as a Term of Art in International Law: The Cyber Operations Context*, 4th INTERNATIONAL CONFERENCE ON CYBER CONFLICT 283, 288 (2012).

²⁸ See e.g. U.S. Department of States Legal Advisor Harold Koh, *International Law in Cyberspace*, <http://www.state.gov/s/l/releases/remarks/197924.htm> - “Yes, international law principles do apply in cyberspace. Everyone here knows how cyberspace opens up a host of novel and extremely difficult legal issues. But on this key question, this answer has been apparent, at least as far as the U.S. Government has been concerned. Significantly, this view has not necessarily been universal in the international community. At least one country has questioned whether existing bodies of international law apply to the cutting edge issues presented by the internet. Some have also said that existing international law is not up to the task, and that we need entirely new treaties to

Some cyber warfare scholars and practitioners use the term ‘cyber-attacks’ because they already assume that those cyber-attacks include kinetic effects, and exclude purely economic effects.²⁹ However, it is also accepted that not all cyber-attacks necessarily result in kinetic effects.³⁰ In this article the term cyber-attacks can be used in conjunction with kinetic or economic, to emphasize the difference and similarity of the two, and to distinguish the two concepts. The various definitions of ‘cyber-attacks’ adopted by different scholars rely excessively on an outdated continuum of effects caused by kinetic weapons. However, this article argues that cyber warfare adds a ‘new slice’ of effects to the continuum, which undermines the common premise that cyber warfare is in fact a phenomenon that is analogous to traditional warfare.

The Joint Chiefs of Staff define cyber-attacks as: “A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an

impose a unique set of rules on cyberspace. But the United States has made clear our view that established principles of international law *do* apply in cyberspace.”

²⁹ See Reese Nguyen, *Navigating Jus ad Bellum in the Age of Cyber Warfare*, 101 CAL. L. REV. 1079, 1089 (2013).

³⁰ See U.S. Department of Defense, Law of War Manual, Art. 16.1.3.2. p. 996 – “The term “attack” often has been used in a colloquial sense in discussing cyber operations to refer to many different types of hostile or malicious cyber activities, such as the defacement of websites, network intrusions, the theft of private information, or the disruption of the provision of internet services. Operations described as “cyber attacks” or “computer network attacks,” therefore, are not necessarily “attacks” for the purposes of applying rules on conducting attacks during the conduct of hostilities. Similarly, operations described as “cyber attacks” or “computer network attacks” are not necessarily “armed attacks” for the purposes of triggering a State’s inherent right of self-defense under jus ad bellum”

adversary's critical cyber systems, assets, or functions".³¹ Other researchers define cyber-war as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption"³² and cyber-attacks as "consists[ing] of any action taken to undermine the functions of a computer network for a political or national security purpose".³³ Other definitions of related terms exist, but so far no universal or even widely accepted definition exists.³⁴

³¹ Gen. James E. Cartwright, Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5 (Nov. 2011). The definition goes on by saying that "The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery."

³² RICHARD A. CLARKE & ROBERT K. KNAKE, *CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT* 6 (2010).

³³ Oona Hathaway, *The Law of Cyber-Attacks*, 100 Cal. L. Rev. 817, 826 (2012).

³⁴ See Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Rand Corporation (2009), p. 179. See additionally Peter J. Denning and Dorothy E. Denning, "The Profession of IT: Discussing Cyber Attack," 53 *Communications of the ACM*, No. 9, at 29, 30, 9/10, which defines cyber-attack as "deliberate actions against data, software, or hardware in computer systems or networks. The actions may destroy, disrupt, degrade, or deny access... Both attack and exploitation require three things: access to a system or network, vulnerabilities in the accessed systems, and a payload... The payload is a program that performs actions once a vulnerability has been found and exercised. A payload may be a bot, data monitoring program,

The scope of the aforementioned definition varies. Some focus on the instrument – a computer, and some focus on the target – computers or computer networks. What is common to all the mentioned definitions is that they exclude the economic effects associated with ECAs as part of the scope of their proposed definitions.

B. ECONOMIC CYBER-ATTACKS

What contemporary definitions of cyber-attacks fail to mention or address is that cyber-attacks can also cause economic effects which are as severe as kinetic effects. To demonstrate this point, consider the following hypothetical: a fighter jet from state A enters into the airspace of state B and bombards a farm along with its field of crops, destroying both completely and beyond repair. There is an evident physical damage – we can see the farm destroyed and the crops are burnt, and the monetary damage caused is quantifiable – in this case – \$500,000. So far, it seems like a kinetic weapon (the bombs attached to the fighter jet) caused kinetic effects (physical destruction of a farm and crops). But now consider this second hypothetical –an ECA intrudes into the computer networks of the main stock exchange of state B, manipulating and erasing information which is worth that same \$500,000. This time there were no kinetic weapons used and there was no ‘boom’ factor, and that immediately

virus, worm, spyware, or Trojan horse; and it is likely to have remote access to the attacker's communication channels. ...An attack payload is destructive, an exploit payload is nondestructive....”

disqualifies that ECAs from being considered just as seriously as the aerial strike was.³⁵

From the effects perspective, both the first scenario and the second scenario resulted in damage totaling \$500,000. In fact, some researchers agree that from this effects-based perspective, such interference with the economic wellbeing of a state is “equated with an armed attack”.³⁶

³⁵ See similar example at William A. Owens, Kenneth W. Dam, and Herbert S. Lin, editors, Committee on Offensive Information Warfare, National Research Council, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 255 (2009): “A cyberattack temporarily disrupts Zendia’s stock exchanges and makes trading impossible for a short period. Bombs dropped on Zendia’s stock exchanges (at night, so that casualties were minimized) would be regarded as a use of force or an armed attack by most observers, even if physical backup facilities were promptly available so that actual trading was disrupted only for a short time (e.g., a few hours). The posited cyberattack could have the same economic effects, except that the buildings themselves would not be destroyed. In this case, the cyberattack may be less likely to be regarded as a use of force than a kinetic attack with the same (temporary) economic effect, simply because the lack of physical destruction would reduce the scale of the damage caused. However, a cyberattack against the stock exchanges that occurs repeatedly and continuously, so that trading is disrupted for an extended period of time (e.g., days or weeks), would surely constitute a use of force or even an armed attack, even if no buildings were destroyed.” Also, See Herbert Lin, *Offensive Cyber Operations and the Use of Force*, 4 JOURNAL OF NATIONAL SECURITY LAW & POLICY 63, 74 (2010).

³⁶ As will be noted in Part 2 of this article, “armed attack” represents the most severe forms of use of force, to which international law permits a response in self-defense. In other words, all armed attacks are uses of force, but not all uses of

As will be argued in the subsequent part of this article, international law provides differential treatment of the two scenarios. The first scenario will be probably classified as a use of force, which is prohibited under international law, however, the second scenario will most likely be something other, lesser than a use of force. It seems that the effects on their own are not the only thing that is taken into account under international law on the use of force, but rather that the means themselves are what matters for the purpose of classifying that act, or that different circumstances accompanying the acts – for example, the use of military weapons, an intrusion into the sovereign airspace of state B and more, are what matters. This distinction does not seem justified anymore in the era of cyber warfare, especially when the economic harm that can be caused by a cyber-attack is so tremendous.

III. THE USE OF FORCE PARADIGM – BLURRY BOUNDARIES

International law has a long history of attempts to regulate the use of force in inter-state relations. The modern framework that regulates the

force are armed attacks. See David Graham, *Cyber Threats and the Laws of War*, 4 JOURNAL OF NATIONAL SECURITY LAW & POLICY 87, 91 (2010), in which Graham rightly argues that: “using this [effects-based] approach, a cyber manipulation of information across a state’s banking and financial institutions significantly disrupting commerce within that state would be viewed as an armed attack. That is, while such an action would bear no resemblance to a kinetic attack, the overall damage that this manipulation of information would cause to the victim state’s economic wellbeing would warrant it being equated with an armed attack”.

use of such force is located in Article 2(4) of the UN Charter, along with customary international law.³⁷

Article 2(4) of the U.N. Charter posits that “All Members 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”. The prohibition on the use of force is a cornerstone of modern international law,³⁸ and is based on the notion that states should resolve their differences in a pacific manner.³⁹ In other words, war is outlawed as an instrument of international affairs, and states should negotiate peacefully to reach an agreeable solution to their mutual problems.⁴⁰

The prohibition, however, is not all there is. There are two exceptions to the prohibition on the use of force – first, if an armed attack occurs against a state, it has a right to resort to self-defense measures, in accordance with Article 51 of the UN

³⁷ Article 2(4) of the U.N. Charter.

³⁸ Christian Tams, *the Use of Force against Terrorists*, 20 EUROPEAN JOURNAL OF INTERNATIONAL LAW 359, 359 (2009).

³⁹ See Article 2(3) of the U.N. Charter, which provides that: “All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered”.

⁴⁰ Preamble of the U.N. Charter reads: “to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest” and “to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest”. Interestingly, this is the only time the U.N. Charter uses the term ‘war’. Other provisions tend to use the terms ‘use of force’, ‘armed force’ and ‘aggression’.

Charter.⁴¹ An armed attack is considered to be the most severe uses of force, meaning that only the gravest uses of force, which are considered armed attacks, invoke the right to military self-defense.⁴² This has been the position of the International Court of Justice, and it represents a wide international consensus on the matter.⁴³ The second exception is UN Security Council resolution under its collective security mechanism.⁴⁴ Under Chapter VII of the UN Charter, the Security Council is authorized take “action by air, sea, or land forces as may be necessary to maintain or restore international peace and security.”⁴⁵ By some, consent of the targeted States is regarded as a third exception to the use of force prohibition.⁴⁶

⁴¹ Article 51 of the U.N. Charter reads: “Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security.”

⁴² The International Court of Justice made a distinction between “the most grave forms of the use of force [those constituting an armed attack]” and “other less grave forms”. See *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Judgment I.C.J.1986, 14, ¶191. This view was reaffirmed in a latter case, see *Case Concerning Oil Platforms (Islamic Republic of Iran v. U.S.)*, Judgment, 2003 I.C.J. 161, ¶ 51 (Nov. 6), available at <http://www.icj.org/docket/files/90/9715.pdf>.

⁴³ Id., See also YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 194 (5th ed., 2011).

⁴⁴ Id., *Dinstein*, p. 305.

⁴⁵ Article 42 of the U.N. Charter.

⁴⁶ See e.g. Ashley Deeks, *Consent to the Use of Force and International Law Supremacy*, 54 Harv. Int’l. L. J. 1 (2014).

Even at this point in time, seventy years after the UN Charter was signed by the drafting state members, the boundaries of the use of force paradigm are still blurry and subject to ongoing debates. Some complicated issues include whether a certain act constitutes a threat or use of force, and whether its magnitude is severe enough to justify self-defense measures,⁴⁷ or what would be a use of force ‘inconsistent with the Purposes of the United Nations’. This article, however, is not intending to answer any of those perplexing questions directly. This article argues that Article 2(4) ought to include economic force demonstrated by ECAs within the confines of its prohibition. The essential determination to support this argument is to explore what ‘force’ within Article 2(4) means, and how can economic force be incorporated in it.

A. *THE MEANING OF ‘FORCE’ WITHIN ARTICLE 2(4)*

The term ‘force’ is a keyword within Article 2(4) of the UN Charter. The use of ‘force’ is prohibited, meaning that to establish a violation there should be a threat or a usage of ‘force’.⁴⁸ One inter-state act could be perfectly legal, while the other is

⁴⁷ That is, in other words, the question of whether a use of force rises to the level of ‘armed attack’ as required under Article 51 of the UN Charter.

⁴⁸ See e.g. Tom Ruys, *The Meaning of “Force” and the Boundaries of the Jus ad Bellum: Are “Minimal” Uses of Force Excluded from UN Charter Article 2(4)*, 108 Am. J. Int’l. L. 159 (2014); Matthew Waxman, *Cyber Attacks and the Use of Force: Back to the Future of Article 2(4)* 36 Yale J. Int’l L. 421, 426-431 (2011); Matthew Waxman, *Cyber Attacks as “Force” under UN Charter Article 2(4)*, 87 Int’l L. Stud. 43 (2011).

not, solely on the premise that one used force, while the other did not.

Article 31(1) of the Vienna Convention on the Law of Treaties sets the most fundamental rule of treaty interpretation.⁴⁹ The ordinary meaning of ‘force’ could be many things. For example, force is defined as “physical, often violent, strength or power” but also as an “organized and trained military group” and “military strength”.⁵⁰ The literal definition therefore varies according to the context.

Many claim that the term ‘force’ excludes economic force as a matter of law, even if the literal interpretation does not exclude it. This argument is often supported by the rejected proposal of the Brazilian delegate to the 1945 San Francisco Conference to include ‘the threat or use of economic

⁴⁹ Article 31 of the Vienna Convention on the Law of Treaties, 1155 U.N.T.S. 331, 8 I.L.M. 679, entered into force Jan. 27, 1980, which reads: “A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose” and “Any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation”. In addition, Article 32 of the Vienna Convention provides supplementary means of interpretation and reads: “Recourse may be had to supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion, in order to confirm the meaning resulting from the application of article 31, or to determine the meaning when the interpretation according to article 31: a. Leaves the meaning ambiguous or obscure; or b. Leads to a result which is manifestly absurd or unreasonable”.

⁵⁰ Cambridge Dictionaries, at <http://dictionary.cambridge.org/us/dictionary/american-english/force>.

measures' as part of the wording of Article 2(4).⁵¹ Although this proposal to amend Article 2(4) was rejected, it does not necessarily follow that it happened due to the belief that 'economic measures' cannot constitute a use of force.⁵² The Belgian delegate, while deliberating on Brazil's proposal, claimed that there is no need for the amendment because the Article already includes a prohibition on uses of force which are 'inconsistent with the Purposes of the United Nations'.⁵³ The Belgian stance is supported by the Report of Rapporteur of Committee I to Commission I, which provided that "unilateral use of force or *similar coercive measures* is not authorized or admitted".⁵⁴ Therefore, the argument that Brazil's proposal was rejected because many already believed that economic force is covered by Article 2(4) is perfectly plausible.⁵⁵ The rejection of Brazil's proposal was not supported by any reasoning at all, so the argument that states did not want 'economic measures' to be considered as uses of force is not necessarily true, and in any way would not be relevant to ECAs which represent a different type of economic force from the one considered by Brazil.⁵⁶

⁵¹ See UN Doc 784 1/1/27, UNCIO Documents 331, 334-35 (1945).

⁵² ADEMOLA ABASS, REGIONAL ORGANIZATIONS AND THE DEVELOPMENT OF COLLECTIVE SECURITY 48 (2004).

⁵³ *Ibid.*

⁵⁴ See Doc. 885, 1/1/34, 6 U.N.C.I.O. Docs. 387, 400 (1945).

⁵⁵ See Abass, *supra* note 47.

⁵⁶ CONSTANTINE ANTULOPOUS, THE UNILATERAL USE OF FORCE BY STATES IN INTERNATIONAL LAW, p. 128. See also D. J. HARRIS, CASES AND MATERIALS ON INTERNATIONAL LAW, 724 (7th ed. 2010) where it is stated that "it is not wholly clear,

Another claim supporting the exclusion of economic force from the scope of Article 2(4) is that the UN General Assembly Definition of Aggression never mentioned ‘economic coercion’ or ‘economic aggression’ as amounting to aggression.⁵⁷ However, due to the non-binding nature of the General Assembly’s resolutions it is unlikely that such resolution is in power to define ‘force’. In fact, ‘aggression’ is used only three times in the U.N. Charter, and bears no significance to the question of whether economic force is ‘force’.⁵⁸

Some refer to Article 51 on the right to self-defense, and point to its words which include ‘armed attack’.⁵⁹ As mentioned earlier, ‘armed attack’ is the most severe form of use of force. The prefix ‘armed’ suggests that only attacks by the use of arms and soldiers could be grave enough to justify self-defense measures. According to this logic, Article 2(4) only includes uses of arms and soldiers, and excludes any other type of force.⁶⁰ In other words, ‘force’ only includes the use of military force.⁶¹ However, Article 51’s usage of the term ‘armed attack’ does not affect the definition of ‘force’ under Article 2(4).

however, whether this was because it was intended not to prohibit economic force or because the term “force” in art.2(4) was thought sufficient to cover it without specific mention”.

⁵⁷ Article 3 of the Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX).

⁵⁸ Rex Zedalis, *Some thoughts on the United Nations Charter and the Use of Military Force Against Economic Coercion*, 17 TULSA LAW JOURNAL 487, 494 (1982).

⁵⁹ Article 51 of the U.N. Charter.

⁶⁰ See Zedalis, *supra* note 53, 493.

⁶¹ See Dinstein, *supra* note 40, 88.

Moreover, the drafters of the UN Charter left no ambiguity in other parts of the Charter, such as Articles 44 and 46 usage of the term 'armed force'.⁶² The preamble, uses similar wording, by providing in paragraph seven that 'armed force shall not be used, save in the common interest.'⁶³

Frequently the narrative of Western states versus developing states is used to demonstrate the 'force' debate.⁶⁴ While the West (mainly the U.S. and its allies) define 'force' narrowly as military attacks, while the developing states define 'force' expansively to include other forms of coercion and aggression as well.⁶⁵ This narrative, however, appears to be changing in the cyber warfare context.⁶⁶ While it is true that historically 'force' was believed to include only military forces, it seems that literally and contextually, 'force' could also include economic force. In the age of cyber warfare, it is even more tempting to include widespread ECAs under the auspices of Article 2(4) of the UN Charter.

Even today, some researchers are convinced that Article 2(4) already prohibits economic and political force.⁶⁷ However, state practice does not offer much

⁶² Articles 44 and 46 of the U.N. Charter, *See also* Zedalis, *supra* note 53, 496.

⁶³ Preamble of the U.N. Charter.

⁶⁴ JULIUS STONE, *CONFLICT THROUGH CONSENSUS*, 87-104 (1977).

⁶⁵ Matthew Waxman, *Cyber Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 *YALE JOURNAL OF INTERNATIONAL LAW* 421, 429 (2011).

⁶⁶ *Ibid*, 436.

⁶⁷ *See* Michael Preciado, *If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect*

support to this argument. It is the core argument of this article that Article 2(4) should prohibit economic force, however, at this time this argument did not yet crystalize into binding international law.

IV. ECA AS A VIOLATION OF ARTICLE 2(4): A LEGAL FRAMEWORK

Some of the disagreement over the prohibition of the use of economic force is because it will entitle victim states the right of self-defense whenever a cyber-attack is causing purely economic harm. Certainly, some ECAs will be so sophisticated and severe that they will be considered armed attacks and invoke the right to self-defense. However, the majority of ECAs will not reach that level. The categorization of ECAs as prohibited uses of force will merely suggest that the attacker is responsible for an internationally wrongful act, and that the victim state has a legal right to reparations for that internationally wrongful act.⁶⁸ As already discussed earlier, there is a certain gap between use of force and armed attack,⁶⁹ and that gap is intended to safeguard the interests of a victim state only when the state is under armed attack, giving rise to self-defense. The main difficulty with regard to ECA is

Critical Infrastructure From Cyber Warfare, 1 JOURNAL OF LAW & CYBER WARFARE 99, 134-135.

⁶⁸ Article 31 of the Draft Articles on Responsibility of States for internationally wrongful acts (adopted by the International Law Commission at its fifty-third session), provides: "1. The responsible State is under an obligation to make full reparation for the injury caused by the internationally wrongful act. 2. Injury includes any damage, whether material or moral, caused by the internationally wrongful act of a State."

⁶⁹ See *Nicaragua v. U.S.*, *supra* note 39.

the evaluation of whether an ECA constitutes a use of force, and if so, if it reaches the level of an ‘armed attack’.

The wording of Article 2(4) and 51 alone do not provide any guidance as to what constitutes use of force or armed attack, even if the event in question is of a purely military nature. States so far have been relying on flexible, ambiguous and somewhat subjective standards to define whether they have been subjected to a use of force.

With regard to cyber-attacks, the normative framework of a use of force assessment is often referred to as ‘Schmitt’s Criteria.’⁷⁰ Michael Schmitt, a prominent researcher of cyber warfare, proposed a seven criteria test to determine whether a cyber-attack is a use of force. Schmitt’s Criteria was later incorporated in the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, which is a nonbinding document created by a group of experts on international law who were invited by the NATO Cooperative Cyber Defence Centre of Excellence at Tallinn, Estonia, that applied contemporary international law to cyber warfare.⁷¹

Although Schmitt’s Criteria does not necessarily limit itself to cyber-attacks that represent *military* uses of force, in the commentary of the *Tallinn Manual* it is pointed out that *economic force* is excluded from the application of the cyber use of

⁷⁰ Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 914-915 (1998).

⁷¹ See Tallinn Manual, *supra* note 10, §11, commentary 9. The *Tallinn Manual* criteria include – severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumptive legality.

force paradigm.⁷² That conclusion, based solely on the rejection of Brazil's proposal, is incorrect.

Certain part of Schmitt's Criteria is well suitable to ECAs as well, but it requires adjustment and removal of irrelevant parts. But before that, ECAs needs to be defined.

The effects part of the framework provided *infra* is the most complex. The consequences of a cyber-attack being considered a use of force and even armed attack are significant, and therefore only the most severe effects should be included within the definition. The severity criterion within Schmitt's Criteria requires "consequences involving physical harm to individuals or property", while it excludes "mere inconvenience or irritation".⁷³ With regards to ECAs the effects have to be more involved with the economic structure of the state or the reasonable economic activity of individuals, however, those effects have to be comparable to physical harm to individuals or property to remain within the stringent confines of the use of force paradigm.

The proposed framework within this article is to provide certain tools to distinguish between economic coercion, which is a form of permissible act in international relations, and economic force, which ought to be prohibited under international law. This distinction has already been impressively articulated by a prominent cyber warfare researcher, which provided that:

⁷² Ibid. Commentary 2 to Rule 11 posits: "whatever 'force' may be, it is not mere economic or political coercion. Cyber operations that involve, or are otherwise analogous to, these coercive activities are definitely not prohibited uses of force."

⁷³ Ibid. Commentary 9(a) to Rule 11.

“Boycotts, the severance of diplomatic relations, the interruption of communications, and economic competition or sanctions between states are lawful and not considered a threat or use of force. In contrast, political or economic aggression [or force] is a use of force within the meaning of Article 2(4).”⁷⁴

In order to evaluate whether a certain action in cyberspace constitutes an ECA, the following non-exhaustive criteria are proposed:

- (1) *Effects magnitude* – this criterion looks to distinguish between the most widespread and serious economic harm from mere inconvenience due to the economic harm. Some cyber-attacks that cause minimal economic harm might be more suitable to be treated by criminal law rather than the use of force paradigm. In such case, a negligible economic harm to a single individual might be considered crime while the shutdown of a state’s stock exchange for weeks would be considered a use of force. However, the effects magnitude will vary from case to case, and it will be only useful to take it into account alongside with the other criteria of this framework.
- (2) *Essentiality* – the more essential the economic activity that is affected, the more likely it is a use of force. To determine essentiality, there must be several factors involved – is the economic activity related to emergency services? Is the economic activity essential to the survival of individuals, such as the ability to purchase basic food products and water? Classic examples that fall under the

⁷⁴ WALTER GARY SHARP, CYBERSPACE AND THE USE OF FORCE 91 (1999).

essentiality scope are the healthcare and justice systems, however, there are additional essential services. If the affected economic activity is not essential, such as purchase of non-essential items online, then it is most likely not to be use of force, but it also varies on a case-by-case basis.

- (3) *State economic infrastructure targeted* – if the economic infrastructure that was targeted and harmed by the ECA belongs to the state or its organs, it is more likely that this is a use of force against that state. It is also possible that there was a use of force in a case of economic infrastructure and activities pertaining to individuals or private entities, but it decreases the likelihood of the ECA to be considered as a use of force, and it will depend on the weight given to the other criteria.
- (4) *Economic nexus* – the cyber-attack in question must be specifically intended to cause considerable economic harm to that state. The purpose of this criterion is to limit the scope of use of force by distinguishing ECAs that were designed to harm the economic affairs and activities of a state from cyber-attacks that did not intend to do so. Generally, intention of the attacker is not considered a requirement in order for the victim to exercise the right to self-defense, but intention is relevant for the requirement of necessity in the self-defense framework,⁷⁵ which requires that a self-defense be

⁷⁵ See Dapo Akande, *Does Use of Chemical Weapons Justify Intervention in Syria?*, EJIL: Talk!, April 27, 2013, <http://www.ejiltalk.org/does-use-of-chemical-weapons-justify-intervention-in-syria/> contending that: “The intention of the “attacking” State should be relevant to whether or not the “victim” has the right to respond in self-defence but this should not be because there is a lack of an armed attack – when plainly arms have been used against that State. The question is whether

the last resort when other methods of dispute settlement have been exhausted.⁷⁶

(5) *Absence of alternative explanation* – the purpose of this criterion is to distinguish between prohibited use of economic force and other types of economic law enforcement or legitimate choice of economic affairs.

(a) *Economic sanctions* – the inclusion of ECAs as a prohibited use of force does not in any way affect economic sanctions. ECAs represent the use of cyberspace capabilities for the purpose of causing harm to a specific state or the entities operating in its territory or under its jurisdiction, and since it is used in a hostile manner, there is no warning before such operation is carried out, nor is it a response to a violation of international law by the victim state. Economic sanctions, especially those provided by Article 41 of the UN Charter, are law enforcement

the lack of intention to attack means that it is not necessary to respond in self-defence. Where there is a genuine mistake then perhaps it would be unnecessary to respond with force. An alternative (diplomatic) solution might be available and thus required by the law. But perhaps lack of intention does not mean that an alternative solution is available (eg the mistaken State refuses to take any steps to correct error and continues to act in ways in which the mistake continues to be repeated or is likely to be repeated). In this case, self defence ought to be available as force is necessary to prevent further uses of force affecting the State.”

⁷⁶ James Green et al., *The Threat of Force as an Action in Self-Defense Under International Law*, 44 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 285, 300-301 (2011).

mechanisms.⁷⁷ The difference between economic force and economic sanctions is the difference between aggression and law enforcement.⁷⁸ The same argument could be

⁷⁷ Article 41 and of the U.N. Charter.

⁷⁸ See Abass, *supra* note 47, where he contends that: “It is submitted that the place of economic force under Article 2(4) does not affect the construction of economic sanctions as enforcements action under Chapter VIII. The legal nature of economic force and economic sanctions under Article 2(4) and Article 53(1) significantly differ. Whereas in the former the issue is whether the use of economic force (which indeed could be in form of sanction) could amount to force under Article 2(4), this is not so under Article 53(1). What Article 2(4) prohibits it the use of force by states in their international relations. What states reject in 1945 is the specific inclusion of economic measures within Article 2(4). Under Article 53(1), economic sanctions are construed, not as an instrument of aggression to invade a state as with Article 2(4), but as a penal measure in response to what the regulating state perceives as previous illegal act by the target state. The difference between the two is the difference between aggression and enforcement action. In legal literature, the distinction is rarely made.” For an opposing opinion, which contends that economic sanctions should, and in fact, are an act of war, see Cassandra La-Rae Perez, *Economic Sanctions As a Use of Force: Re-Evaluating the Legality of Sanctions from an Effect-based Perspective*, 20 BOSTON UNIVERSITY INTERNATIONAL LAW JOURNAL 161, 179 (2002) which eloquently provided that: “From an effects-based perspective, economic sanctions appear to be closer to the use of force than the U.N. has been prepared to admit. Even in the absence of armed enforcement, sanctions forcibly constrain the actions of a nation and may be considered to impinge on that nation's sovereignty. Formerly free to trade with nations willing to trade with it, the target nation suddenly finds itself at the mercy of the imposing force. It finds itself in this position not

used to distinguish prohibited use of military force from measures employed by the UN Security Council under Chapter VII. The first is strictly prohibited,⁷⁹ while the second is permissible because the UN Security Council is authorized to do so as an enforcement mechanism.⁸⁰

- (b) *International trade limitation* – any state can decide on its international trade policies as part of its sovereign prerogative.⁸¹ The question here is whether the economic effects can be explained by a limitation of international trade imposed by an individual or group of states against the alleged victim state.⁸²

always because the nation with which it formerly traded has made a private commercial decision not to trade, but because the former trading partner is compelled either by the U.N. or by a powerful economic force such as the United States to refrain from trade.”

⁷⁹ Unless it falls within the exceptions to the use of force prohibition.

⁸⁰ Article 42 of the U.N. Charter.

⁸¹ See Antolopoulos, *supra* note 51, p. 121. Also see C. EAGLETON, INTERNATIONAL GOVERNMENT 86, 87 (3rd ed., 1957), in which Prof. Eagleton stated: “A state is free to set up almost any barrier to trade and intercourse against one or all states. She may prohibit trade entirely, or in certain articles, or with certain states; she may establish high tariffs against some or all states so far as customary international law is concerned (though there are many treaty limitations).”

⁸² Such limitation, however, will have to conform to international trade law, particularly Articles 1 and 11 of the General Agreement on Tariffs and Trade (GATT).

- (c) *Lack of causal link* – there can be other explanations for the economic harm as well. For example, that the economy in the victim state was already in a bad condition, and that the ECA in question did not directly cause the economic harm, but other activities carried out by the victim state.

Those criteria are non-exhaustive, and it is possible that states will regard additional criteria as necessary in the use of force assessment process. Due to the uncharted waters in which the ship of cyber warfare is currently sailing, it is possible that the changing nature of cyber warfare will require more criteria, and a more nuanced approach to different cyber-attacks in the future.

The application of those criteria to actual ECAs could be tricky at certain times. It is essential to note that the criteria do not provide a definitive answer on whether force was used, but it provides helpful guidelines to be considered in the assessment process.

An example of ECA that would most likely be considered a use of force (or even an armed attack) is an ECA targeting the national bank of State A, causing its computer systems to be disabled for weeks, and therefore any activity of the national bank is disrupted. The effects on the people residing at State A are inability to access or use their bank accounts, including withdrawal of money, which led after only two days to anarchy and chaos. The perpetrators behind the attack are members of the armed forces of State B.

It appears that the effects are a widespread disruption of economic activity, mainly the availability of money and credit cards. This disruption might result in anarchy and chaos because

people in State A would not be able to buy commodities or pay for services. The target of the ECA was a bank belonging to State A, which strengthens the presumption that this is a use of force. The ECA was specifically designed to cause this type of harm, and the effects were a direct result of the ECA. There was no alternative explanation for the attack, it was not a law enforcement operation and definitely not a limitation on inter-state trade.

Another example which leans towards non-use of force is an ECA that shuts down an online shopping website, resulting in temporary inconvenience. This ECA would not be severe enough to qualify as a use of force.

The application of the criteria on an ECA differs from case to case, and depend on all the circumstances of that ECA taken together in the assessment process. At this point, international law needs to abandon its obsolete mindset that economic force cannot be a form of use of force. It can, and it is already here, and now is the time to take action and to send a clear message that such actions will not be tolerated by the aegis of the use of force paradigm.

V. CONCLUSION

This article contends that economic force was initially prohibited by Article 2(4) of the U.N. Charter, and that the literal and contextual interpretation of 'force' within Article 2(4) support this argument. However, state practice and international politics shaped 'force' as to include military force alone. It is possible that customary international law that crystalized over the years following the U.N. Charter conclusion shaped 'force' as including military force only, but this does

not follow the needs of today's world. What was good for states then, is not relevant to the age of cyber warfare, and force today means a different thing entirely. When tremendous economic harm can be caused rather easily, and when this economic harm is equivalent to physical harm in its scale and effects, there is no justification to keep economic cyber-attacks outside of the scope of Article 2(4) anymore. That being said, customary international law might catch up and address the threat posed by ECAs by illegitimatizing them through consistent state practice.

After all, the whole purpose of the U.N. Charter was to "save succeeding generations from the scourge of war", and given that ECAs can represent a new form of warfare, with suffering of innocents involved and potential substantial harm to physical objects, it is time to rethink the dated distinction between physical, economic and political harms, and redraw the boundaries of the use of force framework. Overall, the emergence of cyber warfare requires new, fresh and creative thinking, particularly because international law currently does not provide effective remedies against ECAs.