A UNITED NATIONS CYBER PEACEKEEPING FORCE

excerpt from forthcoming study of
Cyber Arms Control

Edward M. Roche

April 2020

Questions for Reviewers

Instructions

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

1 The United Nations Security Council and its Traditional Role in the Maintenance of International Peace & Security

In Chapter VII of the United Nations Charter details actions that might be taken "with respect to threats to the peace, breaches of the peace, and acts of aggression". This is one of the most important elements of the Charter because it contains the operative treaty language intended to prevent outbreak of another world war. Although the League of Nations had failed to guarantee international peace after the Great War, in the 1945 conference in San Francisco,[1] the United Nations was intended to make improvements to international organization so that peace could be guaranteed. As yet, there has been no repeat of a world war.

The key provisions for keeping international peace should it be threatened are detailed in Charter Articles 39–42. They present an escalating series of steps that ultimately can lead the United Nations to employ military force against a State that has committed aggression.

1.1 Article 42—The Power of the United Nations

Article 42 empowers the United Nations Security Council to "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security". The type of actions that may be taken include demonstration of military power, imposition of a blockade against the offending State, or "other operations". The "demonstration of military power" is the issuance of a warning in the form of a visible display of military force. For example, during a state of tension, it is common for a superpower to move an aircraft carrier or other naval task force into proximity of the source of tension. Military force is not used, but this action becomes a visible showing of the potential force that might be used. The intention is to deter further aggression by suggesting the threat of impending retaliatory

[1] The United Nations Conference on International Organization (UNCIO) took place in San Francisco April 25 to June 26, 1945. It also is known as the "San Francisco Conference".

military attack.[2] Likewise, the imposition of a blockade is an escalation of enforcement action, but it does not involve direct use of military force against an aggressor State. The blockade was used successfully against Germany and very successfully against Japan during the Second World War.[3] A blockade is considered to be an "act of war", but stops short of the actual use of military force.[4] In most cases, it is merely the threat of the use of military force.

Finally, Article 42 allows "other operations by air, sea, or land forces". This is the same as going to war. The only difference is that the prosecution of the war is authorized and controlled by the United Nations Security Council. The functions authorized by the Security Council are either to "maintain" international peace and security or to "restore" it. Maintenance of international peace and security does not necessarily mean engaging in military conflict, but possibly could involve merely the interposition of United Nations military forces between hostile forces so as to keep them from engaging in war. But the "restoration" of international peace and security likely would involve the use of military force (fighting & killing) against one or more belligerents until such time as the fighting is brought to an end.[5] This, then is the most powerful weapon of the United Nations Security Council.

We can say that Article 42 specifies the most extreme action the United Nations Security Council can take. In practice, however, the outbreak of war between nations for the most part is preceded by an extended period of increasing tension, sometimes lasting for months or even years. The Charter is designed so that during this build-up to the outbreak of hostilities, the Security Council has several opportunities to take up the matter and take actions short of use of military force that might help to prevent further escalation and the outbreak of hostilities.[6] The first step in this process of

[2]This is equivalent to the medieval practice during the Inquisition of "showing the tools" to the prisoner before they actually are tortured to make a confession. Often, merely showing the tools would be enough to scare the prisoner into confessing, either truthfully or not. Since that time, justice has improved in many parts of the world.

[3]*See* David French, "British Military Strategy", The Cambridge History of the Second World War, Vol. I, Ferris & Mawdsley, Eds., pp. 28–50 (Cambridge: CUP, 2015)

[4]We assume that the ships blockading a port are enough to deter an attempt to "run the blockade".

[5]According to Edward Luttwak, the purpose of war is to burn out the desire for war.

[6]When the United Nations Security Council begins to consider a potential outbreak of violence, it is said to become "*seized* of the matter".

escalation is found in Article 39.

1.2 Article 39—Determination of Threat to International Peace and Security

1.2.1 Making the Determination

Article 39 of the United Nations Charter is the first step in the process of escalation. It might be called the "Gateway" article. Not every conflict may pass through the gateway. At any time there is an abundance of conflict across the planet. Not every matter has the potential to be grave enough to be taken up by the Security Council. In addition, there are any number of violent events that fall short of threatening *international* peace and security. For example, a change of government within a country leading to violence, even the outbreak of *substantial* violence does not necessarily threaten other countries. In contrast, it is possible to find an increase of tension between two States that is indicated only by the existence of threats, or even the pre-positioning of military forces. There also can be an event that takes place solely within the border of one State that nevertheless can be considered to be a threat to international peace and security. For example, the commission of genocide within a country may not be considered as an entirely "internal matter" falling under the protection of State sovereignty. Consequently, the first step for the Security Council is to screen through the multiplicity of violence around the world and determine which situations might lead to international violence of a nature that should be the subject of its consideration. Article 39 reads:

> The Security Council shall *determine the existence* of any threat to the peace, breach of the peace, or act of aggression and shall *make recommendations*, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.[7]

The principles for determination of whether there is a threat to international peace and security are not entirely defined. For example, what should

[7](emphasis added)

be the determination of the Security Council if a threat to the peace *might* at some time in the future take place, but when for the time being things are quiet? The existence of the Franco Government ("The Spanish Question") was considered in 1946 by the Security Council. Article 39 was considered as regards the "distinction between imminent and potential 'threats to the peace' ". The Security Council *Sub-Committee on the Spanish Question* stated in its June 1st, 1946 report that

> "the activities of the Franco Régime *do not at present* constitute an existing threat to the peace within the meaning of Article 39 . . . nevertheless such activities [are] . . . likely to endanger the maintenance of international peace and security."[8]

The Sub-Committee concluded that the situation in Spain "did not warrant a determination under Article 39"[9], but concluded that it had the potential in the future to do so.

During the same period, the Security Council then went on to consider Greek Frontier Incidents involving "armed bands". In this matter it also was unable to reach a decision leading to the invocation of Article 39.[10] The Security Council noted that violence was occurring because "armed bands" were being formed in one country, then were being infiltrated over the border into Greece and engaging in violence. This was *not* a case of the military forces of one State attacking the corresponding forces of another State.

The Indonesian Question involved hostilities between the armed forces of the Netherlands and the Republic of Indonesia. The matter was complicated by the actions of The Netherlands as the former colonial power. These matters eventually led to the birth of Indonesia as an independent nation.[11] Consideration of the Palestine Question also involved military action, but not between States, like the others.

In the 1960-1963 period, Article 39 was used when Adolph Eichmann was exfiltrated from Argentina to Israel to stand trial for genocide. Argentina

[8] 1946 Repertoire of the Practice of the Security Council 419 (1946–1951) Ch. XI, p. 423, (emphasis added)

[9] *Ibid*, p. 424

[10] *Ibid*, pp. 427–8

[11] For a brief history, *See* Moises Montero de Guzman, *The Indonesian Question Before the Security Council 1946–1949*, M.A. Thesis, Montana State University, 1952

had launched the complaint. The race conflict in South Africa also was the subject of a complaint to the Security Council. Territories in Africa under Portuguese administration as well were subject of concern.[12] South Africa, Portuguese territories and the situation in Southern Rhodesia remained in focus of the Security Council through 1965. These were kinetic conflicts. As the situation in Rhodesia heated up, the Security Council passed Resolution 221 (1966) of 9 April 1966 that declared the situation was a threat to international peace and security. Rhodesia continued to endanger international peace and security.[13] It led to the strong measure of calling for a cut off of petroleum imports. Concerning the situation in the Democratic Republic of the Congo, the Security Council demanded that countries not allow their territory to be used as a base for interfering in the domestic affairs of other states.[14]

In the 1972-1974 period, the Security Council made seven decisions on Article 39. These concerned events in Africa (Zambia, South Africa, territories under Portuguese administration, and Senegal), Latin America, and Cyprus.

1.2.2 Expanding the Scope of Article 39

Over time, the United Nations Security Council has gradually expanded the scope of events that can "trigger" a determination under Article 39. In Figure 1 on Page 11, we see an analysis of Security Council Resolutions from the mid-1940s until approximately 2010.[15] What they show is that the definition of "threat to international peace and security" has been broadened significantly.

In the early days of the United Nations, the Security Council was seized primarily with issues involving military violence. Over time a broader range of disturbances were considered to be threats to international peace and

[12] These areas now are Cape Verde, São Tomé and Príncipe, Guinea-Bissau, Angola, Mozambique

[13] *See* Resolution 277 of 18 March 1970 [Southern Rhodesia]

[14] *See* Resolution 226 of 14 October 1966

[15] Analysis of Resolutions of the United Nations Security Council from the mid-1940s until approximately 2010 show a steady broadening of the range of situations that under Article 39 are considered to be a threat to international peace and security.

security. From the beginning of the United Nations until the mid-1980s, Article 39 was triggered primarily by violent military conflict, usually between the armed forces of one State and those of another. Another source of violence taken up in the Security Council involved the unilateral declaration of independence of Southern Rhodesia. There, the declaration of independence led to military violence with neighboring states. In the period of 1980–1991, the Security Council took up matters involving Israel & Iraq, the Falkland Islands invasion by Argentina, the bitter Iran & Iraq conflict, the Iraq & Kuwait conflict and the crisis in Yugoslavia. In 2000, Article 39 was triggered by the conflict involving Ethiopia & Eritrea.

From approximately 1989, the nature of events that triggered Security Council action under Article 39 changed to focus on civil violence that resulted from a change in government, on ethnic violence, and the threat of terrorism. A change in government caused problems in Lebanon, Liberia, Sierra Leon, Angola and Haiti. Ethnic violence triggered Security Council action as regards Iraq (the Kurds), Bosnia, Sudan and Chad (Darfur). *These were not strictly military conflicts involving armed forces of States as had been the focus in the past.* In the earlier historical phases of the United Nations, ethnic violence and the existence of racism would have been considered to be internal affairs of the nation state and out of scope for the Security Council. During consideration of these matters, arguments were expressed in this vein, but the level of violence and horror seemed too great to ignore. Even though there is a logic to intervention of the Security Council in these types of matters, nevertheless it appears this was a stretch of the language of the Charter beyond its original meaning and purpose. *There is nothing prohibiting the Security Council from so expanding its scope of action.*

After 1990, the Security Council continued to broaden further the types of events that could lead to a finding under Article 39. It made several declarations on the proliferation of weapons, including nuclear, chemical and biological weapons. These declarations were *not in relation to any specific conflict* between States, but instead were an expression of the general notion that lack of control over proliferation was itself a threat to international peace and security. Article 39 was triggered because of violations of an arms embargo (Southern Rhodesia and Somalia), the small arms trade (Srebrenica, Rwanda), ballistic missiles (Iraq).

Again, action by the Security Council had not been triggered by the tra-

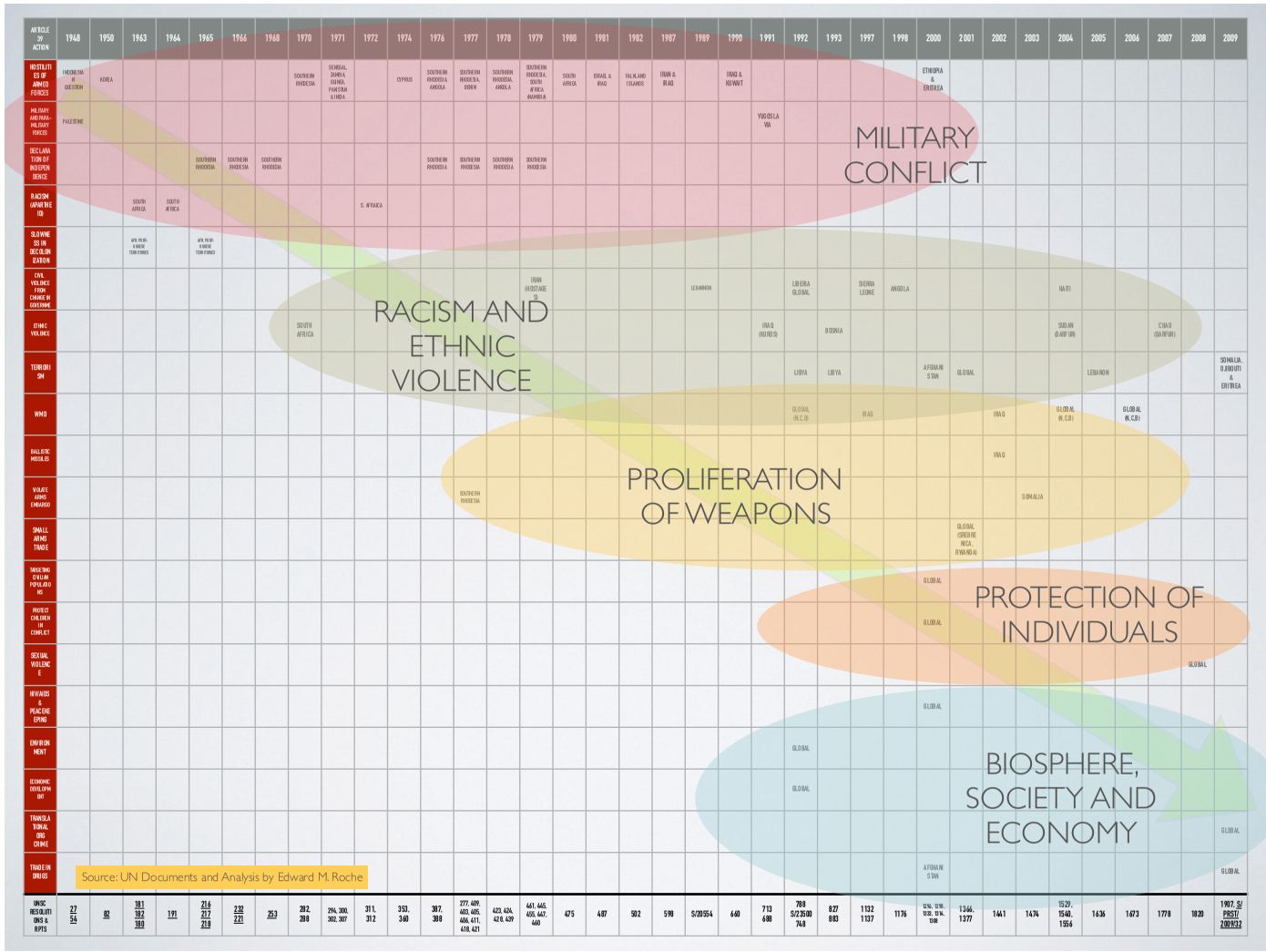

Figure 1: Article 39 Findings of the United Nations Security Council (Mid-1940s—2010) [Full poster available at CyberArmsControl.org] Source: Author analysis.

ditional source of armed conflict between States but instead by the general existence of a global problem. Nevertheless, the type of problem being considered was closely related to the problem of violent military conflict. Again, the range of events that were seen as sufficient to trigger action of the Security Council under Article 39 was being expanded.

By 2000, more than $\frac{1}{2}$ of a century had elapsed since the formation of the United Nations. Again we see a significant widening of the scope of concern for the Security Council. For example, in 2000, it passed resolutions stating that the targeting of civilian populations and the need for protection of children during conflicts could give rise to a threat to international peace and security. In 2008, Article 39 action was found as regards sexual violence. In other words, the existence of a pandemic caused by the spread of a virus could give cause to a threat to international peace and security.[16] Although previous resolutions of the United Nations Security Council generally had related to military violence, even tangentially, the inclusion of a public health crisis appeared to be far out of scope from the original intent of the drafters of the United Nations Charter. Instead of protecting States, the focus of the United Nations had changed to include protection of *individuals*.

During this same period (1990 until the present), the scope of Security Council has continued to broaden. It has made Article 39 findings as regards to damage of the environment, the challenge of economic development, the continued trade in drugs, and the rise of transnational organized crime. All were declared to be threats to international peace and security.

In sum, over time, the United Nations Security Council has increased its definition of what can trigger a finding of threat to international peace and security. At first it was concerned exclusively with military conflict between the armed forces of nations. This certainly was the original intent of the signatories to the Charter. Yet gradually the scope has been broadened to include racism, ethnic violence, general proliferation of weapons, protection of individuals, the biosphere, the world's economy and society as a whole.[17]

[16]In the Spring of 2020, the Covid-19 pandemic crisis did not generate a finding under Article 39

[17]Refer back to Figure 1 on Page 11.

1.3 Article 40—Provisional Measures

In the tower of escalation of actions that might be taken by the Security Council, Article 40 is another firewall that gives the Council an option to take action short of using military force. Article 40 empowers the Security Council to

> [C]all upon the parties concerned to comply with such *provisional measures* as it deems necessary or desirable.[18]

The completion of action under Article 39 is interrupted by Article 40. The Security Council can call for the parties to the hostilities or potential hostilities to comply with provisional measures. Should they decline to do so, it then can make recommendations under Article 39 for further measures to be taken. Articles 39 & 40 serve as a type of notification to belligerents that the international community is watching what they do and has the power to take action if the situation deteriorates further.

The definition of "provisional measures" is not given, leaving this up to the discretion of the Security Council. An example of provisional measures adopted under Article 40 is found in regards to the military conflict between the Republic of Iran and Iraq in the mid-1980s. There, the Security Council called for the parties to "observe an immediate cease-fire", and urged the exchange of prisoners-of-war.[19]

Article 40 specifically states that by taking the provisional measures recommended by the Security Council, no party to the conflict will be considered to have conceded any right, claim or position held in the conflict. The theory behind provisional measures is that negotiation aimed at solving the details of a conflict are intended to come later after the provisional measures have cooled down the temperature.[20]

[18] (emphasis added)

[19] *See* United Nations Security Council Resolution 598 (20 July 1987)

[20] What might be "provisional measures" in the event of a cyber attack?

1.4 Article 41—Call on Member States to Act

If the Security Council has determined there is a threat to international peace and security, then called on the parties to take provisional measures, and finds this has not been sufficient to begin to lower the level of conflict or the threat thereof, then stronger measures may be used.

Article 41 empowers the Security Council to demand that member States take action to *compel* the belligerents to stop their violence. States may be asked to interrupt economic relations with the fighting parties. All transportation and logistics may be cut off. The Charter mentions rail and sea services, because at the time of its drafting, transportation and logistics taking place via air were not commonly used. However, since Article 41 includes the umbrella term "economic relations" then *any* type of transportation would be included such as air-based logistics.

Of particular concern is the option to interrupt postal, telegraphic and radio communications.[21] Although in 1946 when the United Nations Charter was drafted, the Internet was not invented, the inclusion of telegraphic means as a subject of possible interruption by extension refers in today's terms to blocking the World Wide Web.

In particular, Article 41 includes the term "and other means of communication" without specifying, or limiting, the applicability of the Article. By leaving the definition of communication open, the drafters of the Charter allowed for anticipated changes in technology, including development of the Internet.

Article 41 also allows for severance of diplomatic relations as a means of sanction against the hostile parties. If one or more of the belligerents is a non-State actor, then this power in Article 41 has little meaning, because by definition there are no diplomatic relations between parties other than nation States. In practice, the breakdown in diplomatic relations would mean the severing of a communication channel that otherwise might prove useful in exchanging information aimed at bringing to an end the conflict. Even if

[21] In the history of international organization, the term "communication" has undergone a transformation in meaning. Under the League of Nations, the term "communications" referred to postal and telegraphic means, but also referred to what we today call "transportation and logistics". Over time, the term has come to refer to movement of data and information, and not the movement of physical goods or services.

there were a formal breakdown in diplomatic relations, it is reasonable to assume that informal means of contact will persist, if merely for the purposes of conducting negotiations aimed at bringing the conflict to a close.[22]

An additional observation regarding actions by the Security Council is that there are no time limitations placed on these actions. In a practical sense, this means that the Security Council might remain seized of an issue for years, and any provisional or other measures taken might remain in force indefinitely.[23]

1.5 Article 42—Security Council to Take Military Action

If none of the preceding actions by the Security Council prove to be effective, and the situation continues to deteriorate, then the United Nations itself may take military action. This is done through Article 42 which provides that

> All Members . . . make available . . . armed forces . . . necessary for the purpose of maintaining international peace and security.[24]

The obligation to provide military support to the United Nations is not mandatory, but must be done "in accordance with . . . constitutional processes" of the States called upon to supply help.[25] Depending on the State, this implies that enabling legislation might be needed in order to meet the requirements of the United Nations.

The other articles in Chapter VII of the Charter provide details of how military operations by the United Nations will be conducted and how member States will work together to bring about restoration of international peace and security.

---

[22]For example, the Cuban Missile Crisis was solved in large part by the use of an informal "back door" channel of communication between the U.S. President and the Russian Premier. Fortunately the Cuban leader was not involved in their discussions, and was bitterly disappointed when Russia failed to launch a thermonuclear attack on the United States.

[23]We see, for example, that the situation on the Korean peninsula never has been satisfactorily resolved, and technically the nations still are in a state of war.

[24]Article 43(1).

[25]*See* Article 43(3)

2 United Nations Peacekeeping in Cyberspace

There is no legal definition of "global cyber emergency". Here, we refer to an event that has at a minimum the following characteristics: (a) is global in character, having a simultaneous effect on multiple jurisdictions (nations); (b) interferes with critical infrastructure in a way that is substantially harmful to the economy or to the continued operation of important social and cultural activities; (c) the source of the cyber disturbance can reasonably be identified as originating through an intentional interference with cyber space, and thus is not a freak accident or unintended consequence of the world's cyber complexity; (d) is broad and substantial enough to be declared a national emergency by the governments of one or more nation states.

From the analysis *infra* we can conclude that the Security Council is not limited on what it can declare to be a threat to international peace and security. If there is a global "cyber emergency" or the break out of an intense cyber conflict between nations, then what are the current powers of the Security Council under the United Nations Charter? How would it be able to handle this type of situation or would it be powerless? For example, could a "cyber war", "cyber conflict" or "global cyber emergency" be taken up by the Security Council under Article 39? We know this because over time the Security Council has considered issues as general as economic underdevelopment and the environment as being possible threats to international peace and security. This observation must be qualified by noting that although many of those issues, such as the environment and economic underdevelopment have a significant cyber component, here the Security Council was referring to the event itself and not merely to the cyber component.

The lack of any barrier to the broadening of scope of Article 39 was noted by the U.S. Department of Defense:

> There is no requirement that a "threat to the peace" take the form of an armed attack, a use of force, or any other condition specified in the charter. The Security Council has the plenary authority to conclude that virtually any kind of conduct or situation constitutes a "threat to the peace" in response to which it can authorize remedial action of a coercive nature. *Nothing would prevent the Security Council from finding that a computer*

> *network attack was a "threat to the peace"* if it determined that the situation warranted such action. It seems unlikely that the Security Council would take action based on an isolated case of state-sponsored computer intrusion producing little or no damage, but a computer network attack that caused widespread damage, economic disruption, and loss of life could well precipitate action by the Security Council.[26]

Here we are more specifically concerned with a scenario in which one nation attacks another using cyber weapons, and the question of whether the UN Security Council becomes seized of the matter. Can the United Nations deploy a "Cyber Force" in response?

Below is a *scenario* showing how the United Nations Security Council might respond to a global cyber emergency. The objective of presenting a scenario is to examine the rules in place and see how they might be exercised in handling a cyber emergency. It is argued that although a "United Nations Cyber Force" does not exist, under the current rules there is nothing in the Charter to prevent its formation.

2.1 Bringing a Cyber Emergency Before the Security Council

2.1.1 Appreciating the Level of Severity of a Cyber Attack

The first level of consideration is assessing a cyber emergency as being important enough to be taken up in the Security Council. We may envisage a number of cyber emergency scenarios that could be serious enough to be brought to the attention of the Security Council.

Usually, as a matter or protocol, an issue is brought to the Security Council through a letter originating in from a member State and addressed

[26]Phillip A. Johnson, Office of General Counsel, Department of Defense, An Assessment of International Legal issues in Information Operations, Second Edition, reprinted in Michael N. Schmitt and Brian T. O'Donnell (Eds.) *Computer Network Attack and International Law*, 76 International Law Studies 480, 459–529, November 1999 (emphasis added)

to the President of the Security Council. This can occur under two conditions. First, the originator of the letter can be one of the belligerents. Second, the letter can originate from an interested Third Party, such as a neighboring State that might fear being brought into the conflict. This first requirement acts as a screening mechanism to filter out a large number of cyber incidents.

The decision by a national government to bring a matter to the attention of the Security Council is problematical for several reasons. First, a distinction must be drawn between attacks against private sector interests in a nation and attacks against the government itself. The party petitioning the Security Council must have standing. For example, if a multinational enterprise or any other party in the private sector is the victim of a cyber attack, it does not have standing to bring the matter to the attention of the Security Council. Only its government as a representative of its interests might do so.

Using severity as a guage, the vast majority of cyber attacks against private enterprise likely would never lead to a nation approaching the Security Council. Attacks against private interests generally are not considered to be attacks on the nation State in which they reside unless the effect of the attack has broader downstream consequences for the society as a whole. On the other hand, when cyber attacks are launched against the government itself, then this is closer in effect to a kinetic military attack and without doubt is seen as aimed directly at the nation State itself, even if technically less extensive than a private sector attack.

Here, there is an analogy with international law, and in particular the laws of war and humanitarian principles. It is generally unacceptable to engage in wanton military attacks against unarmed civilian populations. These rules occasionally are observed by belligerents. In the same way, when engaging in cyber conflict, the analogy would be that it is not permissible to engage in cyber destruction of civil society.

It should follow that the only condition in which a nation would launch full-scale cyber attacks against another nation's general infrastructure or civil society interests is when the conflict might be serious enough to threaten the survival of one of the States or its vital interests.

It also may be necessary to distinguish between a sudden "out-of-the-blue" cyber attack and a continuing series of smaller attacks that perhaps

are increasing in severity, but at any one point in time do not rise to the level of catastrophic damage. Although there is no barrier to placing this type of matter before the Security Council, it is less feasible. It should be recalled, however, that there are no specific rules binding a decision of the Security Council to take up a matter. It can declare *any* event to be a threat to international peace and security.

If there were a period of heightened tensions between two States, then as part of an increase in tensions, one State might launch a cyber attack against the private interests of the other party. If that happened, and the damage was severe enough, then the receiving State would be justified in bringing the matter before the Security Council. Here, it would not be the level of cyber-induced damage that is the deciding factor in making the matter important enough to receive Security Council attention, but instead the overall context of a wider range of antagonistic touch points that makes a broader conflict more probable. This means that the size or extent of a cyber attack is not always an independently sufficient condition necessary for the matter to be taken up by the Security Council.

If the cyber attacks were taking place as part of a broader military conflict involving *kinetic* force, then the cyber dimension would be viewed as merely an extension of the broader military conflict. In that case, instead of moving to specifically isolate cyber as part of the conflict, the overall breach of the peace would be placed before the Security Council. We can expect that when cyber attacks are carried out in support of kinetic military operations, then the Security Council will default to consideration of the military conflict using its historically traditional pattern of governance.

In sum, a cyber attack launched by one State against another might rise to a level of severity so as to justify taking the mater before the Security Council if the attack were against the government infrastructure of one party or it was an attack against private sector (civil society) targets within a context of heightened hostility and tension between the two parties.

2.1.2 Managing the Attribution Problem

A further complicating factor serves as a barrier to approaching the Security Council. It is the attribution problem. As a consequence of suffering a

cyber attack, any State making a request for Security Council intervention must be sure of its origin. Attribution is less of a challenge in conventional warfare. For example, in the Cuban Missile Crisis, initial discussions started with Russia and Cuba denying the existence of the missiles and soldiers that were being set up in Cuba. It was only when the U.S. Representative to the United Nations dramatically revealed photographic evidence of the rocket installations that these propagandistic denials withered. The speech was given by Adlai Stevenson in the Security Council October 25, 1962.

> "I want to say to you, Mr. Zorin, that I do not have your talent for obfuscation, for distortion, for confusing language, and for double-talk. And I must confess to you that I am glad that I do not!"

In the lead up to the First Persian Gulf War, the U.S. Representative, Colin Luther Powell presented to the Security Council transcripts of intercepted telephone conversations purporting to show discussions regarding placement of Weapons of Mass Destruction.[27] Both of these demonstrations had a dramatic effect on the deliberations in the Security Council.

But in case of a cyber incident, it might be meaningless to come into the Security Council with photographs. If so, then what type of dramatic proof could be provided? It is almost comical to see a Representative to the United Nations standing before the international body giving a demonstration on computer code. Nevertheless, we must assume that a member State would have its reasons for attributing the cyber attacks to a specific origin.[28] Although there would almost certainly be denials on the part of the corresponding belligerent, the severity of the situation would be visible for

[27] *See* United Nations Press Release, Briefing Security Council, US Secretary of State Powell Presents Evidence of Iraq's Failure to Disarm, SC/7658, 5 Feb. 2003, 4701st Meeting (AM) (It turned out later that the conclusions drawn from this evidence were not accurate.)

[28] *See* Jon R. Lindsay, "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack", 1 J. of Cybersecurity 53–67, 2015 "Cyber attackers rely on deception to exploit vulnerabilities and obfuscate their identity, which makes many pessimistic about cyber deterrence. The attribution problem appears to make retaliatory punishment, contrasted with defensive denial, particularly ineffective."; *see also* Nicholas Tsagourias, "Cyber attacks, self-defence and the problem of attribution", 17 J. of Conflict and Sec. L., 229–44, 2012 "[T]he victim State can use force by way of self-defence against another State if the attack has been committed by the latter's organs or agents

all to see, particularly if the targets of the attack involved important public infrastructure such as the equities markets, electronic trading systems, medical facilities, or transportation networks. In order to make the case for intervention, not computer code, but instead evidence of the destruction, disabling or other damage to these systems would be part of the evidence presented to the Security Council.

It is almost certain that the corresponding belligerent would deny responsibility, and place the blame elsewhere. There would be no way immediately for the Security Council to resolve the contradictory accounts of the events at hand. Here, however, we are concerned only with meeting the threshold to approach the Security Council. Consequently, *it would be possible for the Security Council to become seized with any cyber incident even without complete resolution of the attribution problem.* It should be recalled that measures taken by the Security Council can be made without prejudice to the rights or claims of either side in a conflict. This lowers the barrier to Security Council consideration of a potential conflict. In sum, the attribution problem is no barrier to consideration by the Security Council.

2.2 Article 39—The Security Council Becomes "Seized" of the Cyber Emergency

After one of the belligerents or a third party invites consideration by the Security Council, there still is no obligation for it to act.[29] At this point, a number of considerations would determine whether the Security Council becomes "seized" of the matter.

Often, disputes are brought to the attention of the Security Council, but are not considered grave enough to be declared a "threat to international peace and security". It frequently has happened also that one of the Permanent Members of the Security Council quickly vetoes further consideration of the matter. For example, during the Cold War, it was common for one

---

or has been committed by non-State actors tolerated by that State.";Thomas Rid & Ben Buchanan, "Attributing Cyber Attacks", 38 J. OF STRAT. STUD. 1–37, 2015; David A. Wheeler & Gregory N. Larsen, 'TECHNIQUES FOR CYBER ATTACK ATTRIBUTION, Alexandria, Va.: Institute for Defense Analysis, Paper P-3792, 2003

[29]The Security Council is not required to take up every matter brought to its attention. This is not unlike the process of *certiorari* for the U.S. Supreme Court

or the other super-powers as regards matters they considered to be taking place within their sphere of influence actively to *prevent* its consideration in the Security Council. In a cyber stability scenario, it is reasonable to predict that should the cyber attacks be originating from one of the Permanent Members, the matter will *never* be placed before the Security Council.

Under Article 39:

> "The Security Council shall determine the existence of *any* threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security."[30]

The qualifying term "any" presumably means that if a non-kinetic cyber emergency was severe enough to threaten international peace and security, then it would qualify for consideration. One problem to note is that the term "peace" is not clearly defined. In classical national security terms, "peace" refers to the lack of military ("kinetic") conflict between belligerents. No one ever has defined "cyber peace" or "cyber stability".

How could a cyber event lead to action by the Security Council under Article 39?

2.2.1 Kinetic Response to Cyber Attack

There are two variations of how a cyber incident could be a threat to international peace and security. First is a scenario in which the severity of cyber attack is enough to cause the corresponding party to launch a military "kinetic" attack in retaliation, so as to stop the cyber attack. If the responding nation State launched a kinetic counter-attack, such as by dropping bombs on the computer facilities responsible for origination of the cyber attack threatening its sovereignty, then it would quickly ease the barrier to Security Council consideration of the matter.

A vast amount of ink has been spilled discussing whether a cyber attack which causes no *physical* harm, but only *informational* harm, can justify

[30] (emphasis added)

military *kinetic* retaliation. For a while, there appeared to be a type of barrier to such a response, based on customary international law. However, in May of 2019, in response to a cyber attack launched from the Gaza administrative zone by the Hamas organization, Israel launched a military "kinetic" counter-attack to destroy the servers and other technology used to launch the attack.[31] This answers the question of whether a cyber *informational* attack can give rise to a "classical" military response.

So under this new historical precedent, there now is less of a barrier for the Security Council in finding a threat to international peace and security originating solely from a cyber attack. A complication occurs if the corresponding belligerent has no prospects of launching a kinetic counter-strike against the State responsible for the cyber incident, or if the level of cyber attack is below the threshold needed for one belligerent to justify a kinetic response. In that case, the threat to peace must be interpreted as meaning a "threat to cyber stability". Here, the Security Council would need to find that the level of cyber disruption was so severe as to merit its attention. This might prove to be a major barrier to consideration. We only can conclude that should the demonstrated effects on society be substantial enough, it would make it easier for the Security Council to make a positive finding.

What is the practical result as regards a cyber incident? It is clear that even if the incident did *not* have a kinetic component, nevertheless, it could be serious enough to attract the attention of the Security Council and if there were significant agreement, then it could be declared as a "threat to international peace and security". The only barrier to such a declaration would be the disagreement of any permanent member of the Security Council. This would happen only if either the source of the cyber attack was one of the permanent members, or if the attack originated in a client ally State.[32]

It also is possible to draw a distinction between the *effect* of the cyber attack upon the society and population of the victim state compared to the effect on its cyber infrastructure. In one case, a cyber attack may harm only a

[31] *See* Catalin Cimpanu, "In a first, Israel responds to Hamas hackers with an air strike", ZDNet (online) May 5, 2019

[32] Or if one of the permanent members did not wish to set a precedent for Article 39 action in this type of non-kinetic scenario. Such a reluctance might be present if there was a worry that such action might curtail the freedom of action in the future in cyberspace for the permanent member.

restricted portion of the cyber infrastructure of the victim State, but generate substantial harm to the lives of its citizens. For example, a cyber attack targeting the distribution of drinking water may do little physical damage, but generate extreme disruption throughout a society. On the other hand, a cyber attack might have a substantial effect on informational resources within the victim State, but fail to have a significant effect on the lives of individual citizens, at least in the short term. For example, the national archives might be erased, or the access to property records might be suspended, or banking information might be disrupted. This type of informational attack would not kill persons, but still could be severe enough to cross the threshold needed under Article 39 by the Security Council.

It should be noted that under the language of Article 39, there is no requirement that international peace and security be breached, only that there is a *threat* of it being breached. Unless the demonstrated level of damage suffered by the victim member State was convincing, the issue would not pass through this screen towards consideration by the Security Council. In the absence of any tangible evidence of harm, it would be difficult for the Security Council to make a determination that certain cyber activities were a "threat". How would it do this? This leads to the conclusion that the Security Council would most likely find a threat to international peace and security when it was shown evidence of abusive cyber activities of such a magnitude that they threatened a military "kinetic" response from another party.

2.2.2 Defining a Cyber "Breach"

The second type of triggering condition found in Article 39 is a "breach" of the peace. We know that in the original design of the Charter, this refers to the outbreak of hostilities—people start shooting at one another or blowing things up. This has never been defined for cyberspace. There is, however, no need for a conclusive agreement on a binding definition of cyber "breach" because a breach is what the Security Council determines it to be.

This likely would be determined by the effect. For example, if a cyber attack froze the financial system, causing significant economic disruption, this almost certainly would qualify as a breach of the peace. It is true that

Finding	Condition Variation
Threat	Indications of an impending cyber disturbance that could interfere with cyberspace (Internet and cloud-based ICT services) in victim member State. Type of threat giving rise to a conventional military "kinetic" response.
Breach	Cyber disturbance that interferes with cyberspace (Internet and cloud-based ICT services) in victim member State. Breach of kinetic peace with a significant supplementary cyber component in hostilities.
Act of Aggression	Similar to breach except that it is possible to clearly identify the party initiating the violence.

Table 1: Variations of Possible Findings of the Security Council under Article 39 of the Charter.

as of this time[33] the Security Council has never made such a finding. But there never has been a major catastrophic cyber attack against the private sector of one member State that definitively can be attributed to another member State and was of such severe effect that it might merit consideration by the Security Council. In this part of Article 39, the Security Council has the option to become seized with a matter without making any determination as to attribution; it only is necessary that the level of cyber disturbance be great enough to merit international attention.

2.2.3 Cyber Act of Aggression

In the third level of Article 39, the Security Council finds there has been an act of aggression. This assumes it is possible clearly to identify the member State responsible for the aggression. It also presupposes that whatever violence is being promulgated is not reasonably in accordance with the self-defense provisions of Article 51, but instead is not justified. In a cyber aggression scenario, it would be required for the Security Council both to become aware of a serious breach to cyber stability, and have clear indications of the source and thus the responsibility for the cyber attack.

[33] July of 2019

In this connection, a problem arises if the originating member State territory is the loci of the cyber attack, but the parties conducting the attack are not part of its government. Here, there are two variations. In the first variation, the malicious cyber work is being conducted by parties that are *not* authorized by the member State government. An example would be if a group of paid hackers and computer criminals were interfering in the stock market of a foreign nation in a way so as to give opportunities for investment or other financial activities to rogue traders or other criminal syndicates. In this variation, the attribution problem is partially solved, because the identity of the originating member State is known. In a second variation, the malicious computer work is being performed by vigilante groups who have either the active or passive support of their government. Active support by the member State government would come in the form of financial incentives or other enabling resources including legal protection[34] being provided by their government. Passive support would be found when the member State government is not actively supporting the malicious cyber activities, but at the same time is aware of them yet has a policy of not preventing them.[35]

So even if it is not possible definitely to make conclusions regarding the responsibility of the cyber attacks, still there is no barrier to the Security Council becoming seized of the matter. The only gating factor is the level of cyber disturbance and an assessment by member States that the damage is severe enough or *might* become severe enough to merit its attention. For the Security Council, severity of damage either realized or potential is a more important factor than attribution, which is not a condition precedent for a decision under Article 39.

2.3 Article 40—The Security Council Recommends Provisional Measures to Prevent Further Cyber Destabilization

If the Security Council becomes seized of a cyber matter, then it has the option to take action under Article 40; it can make recommendations that hopefully will prevent the situation from getting worse. At the core of every

[34]Example: Exemption from prosecution for computer crimes.

[35]This is sometimes referred to as "plausible deniability", but increasingly has grown thin as a believable defense.

conflict between nation states, usually there is a source of the problem, and disagreement regarding how to get it resolved. In its activity under Article 40, the Security Council is not concerned with the minute details of the conflict, but instead is concerned primarily with stopping escalation of violence.

In doing this, it can call on the parties to take "provisional measures" to lower the temperature of the emerging conflict. In kinetic conflicts, this might mean a cease fire. In a cyber conflict, it might mean a temporary cessation of malware attacks, or the restoration of ICT services that may have been disrupted.

A related problem arises in addressing the challenge of vigilante groups or government "subcontractors" who may be involved in cyber attacks. Under the assumption that it has been established with reasonable certainty that the attacks originate within the territory of a specific member State, but that State's government has declined responsibility, and yet the attacks are enough to cause the Security Council to become seized of the matter, then it might define a provisional measure that requests member States to take such measures *internally* to ensure that the situation is not worsened. In other words, if the cyber disturbance was being caused by vigilante groups, then the Security Council would call on the member State to send in its law enforcement to stop their activities.

There are a number of options available for preventing further cyber escalation by vigilante groups. These include: (a) arresting or detaining the individuals responsible for the cyber attacks; (b) forcing telecommunications or Internet service providers from extending services to same; (c) using deep packet inspection or other techniques to filter out-going cyber attacks; (d) issuing a temporary restraining order against various entities in order to accomplish the same objective; (e) bombing or otherwise destroying offending illicit cyber bases; (f) bombing or otherwise killing the cyber terrorists.

It also would be possible for the Security Council to ask other member States to take actions that might restrain the level of cyber hostility. Examples of this type of action would be a request that Internet Service Providers within their jurisdiction take actions to prevent further cyber disturbances from transiting their networks. Generally, however, provisional measures are aimed at the belligerents themselves, as specified in Article 40.

Since there is no time schedule associated with compliance to Security

Council recommendations for provisional measures, it is not possible to know how long this phase of the conflict would continue. The most important factor to consider would be the level of cyber damage that continues to be inflicted. The record indicates that the Security Council may become seized with a matter for *years* at a time.

2.4 Article 39—The Security Council Makes Recommendations

Depending on what happens as a result of the provisional measures that may be considered under Article 40, the Security Council has the option of either doing nothing and simply remaining seized of the matter, or taking further measures. It is possible that the result of the provisional measures is positive, and the level of cyber violence will decrease, and mechanisms including diplomacy will be able to lower the level of tension. In addition, it is possible that a member State under cyber attack might be able to put in place cyber-security measures that are robust enough to curtail the damage other belligerents are attempting to inflict.

However, if we assume that the provisional measures are ineffective, or that one or more of the member States refuses to comply, and that the level of tension caused by the cyber emergency continues to increase, then the Security Council can make recommendations on what should be done, or can move directly to taking action under Articles 41 and 42.

In practice, and by custom, the Security Council first makes recommendations directly to the belligerents. These recommendations are by no means the statements of a "paper tiger", for they are backed by the entire authority of the Security Council and in order to be made require the support of all Permanent Members of the Council. In many cases, one or more of the Permanent Members will abstain from voting on an action by the Security Council. When this happens, it still is possible for the recommendation to pass. By not disagreeing directly with the recommendation through use of its veto, the abstaining Permanent Member is signalling that although it is very much concerned with the matter, it will not necessarily support stronger action of the Security Council that might be suggested under Articles 41 and 42.

There is a great deal of flexibility in the types of recommendations that can be made by the Security Council. It should be noted that whereas in Article 40, the instructions regarding provisional measures are made with respect to the belligerents, under Article 39, recommendations can be made to *any* party, that is to *any* member State.

In this scenario, we are assuming that the nature of the instability is a cyber-based conflict, and there are no kinetic forces involved. In seeking to contain a cyber emergency, the Security Council could recommend that each belligerent engage in a "cease fire", or cooperate with each other in exchanging information so as to lower the level of tensions. But the Security Council also could recommend that other member States take actions to stop the cyber emergency. This might include measures such as (a) preventing the travel of programmers; (b) stopping the export of information services; (c) ceasing access *on their own territories* to ICT infrastructure that might be used by the belligerents to conduct cyber attacks; (d) engage in monitoring of the Internet in order to understand the level of compliance with Security Council Resolutions.

As in the case of provisional measures, the Security Council would engage in monitoring the cyber emergency to assess the level of compliance with its recommendations. Again, the amount of time to wait to see if the measures have any positive effect in mitigating the level of cyber violence is not specified. Consequently, whether or not the Security Council moves to take up further action under Articles 41 & 42 will depend on the level of cyber carnage the belligerents inflict on each other.

In the historical and traditional world of kinetic conflict, it is a formidable barrier for the Security Council to move to take action under Articles 41 & 42. Traditionally, this involves violence, use of military force or the threat thereof, and war-fighting, with all of the dangers of a conflict spiraling out of control. Therefore, historically, there is a strong reluctance on the part of the international community to allow the Security Council to become engaged in this type of action.

In contrast, the nature of cyber conflict leads to a completely different result. Two forces will be at play that will *increase* the probability that the Security Council will more rapidly move to further action under Articles 41 & 42. First, since cyber conflict for the most part will not be aimed at the destruction of human life, and will not be based on kinetic effects, then fear

of untoward consequences of Security Council action will be decreased. *Without potential kinetic effects, there is a lower barrier to entry for use of cyber power by the Security Council.* Second, the sense of urgency will be much greater because of the inter-connected nature of the world's telecommunications infrastructure. In cyberspace, the danger of a conflict breaking out and causing a chain reaction across the cyber infrastructure of the entire planet hypothetically is much greater than is the danger of a regional kinetic conflict spilling and causing a larger military confrontation. Consequently, given the inter-connected nature of the Internet world-wide, there will be a severe risk that any malware tools being used in the cyber attacks will become released into the global Internet ecosystem, leading to increased collateral danger for member States at the time not involved in the cyber conflict. Whereas in the case of a kinetic conflict, even though there always is a chance of it *gradually* spreading, in the case of a cyber emergency, it is possible for devastating consequences to be promulgated over night.

Appreciation of this danger will force a considerable speeding-up of the decision-making processes in the Security Council. To a certain extent, this might indicate an increased risk of poor decisions being taken. However, this risk must be balanced against the fear of global consequences to cyber stability if prompt and effective action is not taken. Cyber stability may be more fragile than kinetic stability.

2.5 Article 41—Security Council Uses the Internet "Kill Switch"

In this Article, the Security Council does not take action itself, but instead can "call upon Members of the United Nations" to take measures that will "give effect to its decisions". The exact wording of Article 41 is:

> The Security Council may decide what measures *not involving the use of armed force* are to be employed to give effect to its decisions, and it may *call upon the Members of the United Nations* to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, *postal, telegraphic, radio, and other means of communication*, and the

severance of diplomatic relations.[36]

Of particular concern for management of cyber stability is the power to call for "complete or partial interruption" of communications. This means that the Security Council has the power to call for a State to be completely cut off from the Internet. All social media, email, e-commerce, cloud services, banking transactions, even telephone communications and encrypted apps such as WhatsApp or Line would be closed down.

In an advanced nation, such a shut down would be equivalent to a cyber "atomic bomb", only for the entire society at once. This is an extremely severe measure, and it is doubtful that any nation today could survive such a shut off.

The flexibility to call for "partial" interruption has important implications for management of cyber stability. In practice it means that for any social media, cloud service, email, or other application that has any lever of control actionable from outside of the member State, it would be possible to *selectively* apply the restrictions.

2.5.1 Cyber as a Precision Weapon

Cyber may be the most precise weapon ever invented. For example, it would be possible to block the communications of everyone except IP addresses originating from medical facilities. It would be possible to block the Internet communications of persons from one city but not another. It would be possible to block all Internet communications from IP addresses originating with the government or military establishment, but leave open the communications of Civil Society. If there were civil disturbances, it is reasonable to expect the capability of turning off all Internet communications of government personnel, but leaving open all Internet communications of dissidents, or of those attempting to overthrow the government. Or the other way around—the communications power of the government could be left in tact but the citizenry could be turned off. If there were specific companies, organizations, or economic sectors to be targeted, then it should be possible to selectively target them as well, leaving untouched and uninterrupted other sectors.

[36](emphasis added)

What is the result? *The practical effect of the Internet and the revolution in cyberspace has been a vast increase in the power of the Security Council.* This is because in the original framing of the UN Charter, Article 41 envisages simply cutting off or interrupting telecommunications traffic in to and out of an offending nation State. With the penetration of social media, cloud services, digital certificates and other aspects of the Internet throughout more or less every nation, the level of inter-connectedness has vastly increased.

Some nations, most notably China and Russia, have done much to build their own infrastructure for an Internet separated or separable from the rest of the world. In the case of China, there was a dual purpose: First, to copy the technologies of the West without paying excessive royalties for intellectual property; Second, to increase the power of the national government, since it has ultimate sovereignty over all information within its jurisdiction.[37] But even in the case of China, it would suffer greatly if its corporations were cut off from the outside world. The same is true of Russia or of any other nation that has attempted to build informational autonomy into its national security strategy. The United States is equally vulnerable, but may enjoy an advantage over other nations because so much of Internet technology and communications is owned by its companies.

In some nations, in-country data processing requirements have been enacted into law. This requires providers of Internet-based cloud services to ensure that name-linked data connected to any of its citizens be stored and processed *within* the country. This presumably means that should there be a cut-off from the outside, the personal data of its citizens would not be compromised. Even so, it is not clear that given a cut-off of services, these home-based information systems would continue to operate. Apart from some experimentation in Russia,[38] there has been little reported regarding

[37] It is guided by the doctrines of the Communist Party.

[38] *See* Taylor Hatmaker, "Russia plans to test a kill switch that disconnects the country from the Internet", TECHCRUNCH (online), 11 February 2019; Zak Doffman, "Putin now has Russia's Internet kill switch to stop US. cyberattacks", FORBES (online) 28 October 2019; Thomas M. Chen, "Governments and the Executive 'Internet Kill Switch' ", IEEE NETWORK, March/April, 2011, p. 2; Karson K. Thompson, "Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate", 90 TEX. L. REV. 465 (2011-2012); Scott M. Ruggiero, "Killing the Internet to Keep America Alive: The Myths and Realities of the Internet Kill Switch", 15 SCI. AND TECH. L. REV. 241 (2012); David W. Opderbeck, Does the Communications Act of 1934 Contain a Hidden Internet Kill Switch, 65 FED. COMM. L.J. 1 (2013); Deborah Beth Medows, The Sound of Silence: The Legality

actual field testing of this type of emergency situation. Therefore, the global effects of such a cyber event are unknown, and unpredictable.

In the same way the possession of nuclear weapons has made obsolete the notion of war between the superpowers, it is unlikely there will be a major cyber war between the world's cyber superpowers. As a result, the Security Council will most likely become seized of matters involving cyber conflicts between states that are not cyber superpowers. In this aspect, cyber is not unlike kinetic.

2.5.2 The Private Sector Problem

Another complicating factor in the use of Article 41 action is the relationship between government and the private sector. Almost all social media, cloud services and other Internet application platforms are owned and operated by the private sector. Consequently, a gap may emerge between government policy and what private enterprise is willing to do. For example, it is not clear that multinational enterprises would wish to be seen going forward as mere tools of government policy. An example would be Apple Computer's resistance to demands from the Federal Bureau of Investigation in the U.S. to provide tools to break the security of the encryption system used by its customers. Since providing privacy is an important feature making Apple products attractive to the consumer, giving up that privacy for all of its customers likely would have serious untoward consequences for Apple's business. There would be immediate concern regarding the long-term effect on their business in those nations against whom they were forced to take action. The reputation effect of close cooperation with a national government can be severe and have an effect on the goodwill and thus stock price of a company. In a nation such as China, a multinational's long-term business interests might be greater than their future in the United States, and this would be another reason to avoid following orders from the U.S. government. In addition, if selective measures were used, such as cutting access and services to some persons or organizations and not to others, then it would reveal the level of confidential and personal knowledge the service provider has accumulated regarding its customers.

---

of the American "Kill Switch" Bill, 4 J. of L., Tech & the Internet 59 (2012)

It is without doubt that such enforcement action would dramatically reduce the trust in these cyber entities. A similar breach of trust occurred when it was reported that the U.S. National Security Agency (NSA) had compromised the systems of the major email providers such as Google Gmail, Yahoo mail, and Microsoft's Hotmail. This had been done with full cooperation from the corporations providing the service. The result was a substantial drop in the confidence held for the security of U.S. based cloud services. As a result, the European Union started to take measures to ensure that those services were provided to European citizens only from computer centers based in Europe, out of the jurisdiction of the United States.

In the United States, absence a declaration of war, there is no established mechanism in place that would allow the U.S. government to agree to cyberspace enforcement activities for the Security Council and then *automatically* have those activities carried out by the private sector. One solution to this problem would be to put in place enabling legislation to compel social media, cloud, and other Internet service providers to follow governmental instructions if the authority came from the Security Council and was agreed upon by the U.S. government.[39] Generally, it is U.S. policy to conduct its affairs in a way that does not contravene recommendations of the Security Council. This type of automaticity would be the route in many countries which the government has a more commanding power over the business sector, or is a co-owner.[40]

The United States presents a contrast. In the United States, it would be extremely difficult to get such "automaticity" legislation passed. One only can imagine the furor that would be generated if the U.S. Congress took up consideration of a law that would require Facebook, Google, Apple, Microsoft, IBM, AT&T, Verizon and others to be manditorially bound to carry out any cyberspace policy agreed to by the U.S. in the Security Council.

Business organizations most probably would oppose the measure and predictably launch a public relations campaign along the lines that it is not a good idea to let international organizations controlled by others "dictate" to U.S. business specific things to do in their *internal* operations. The debate would fracture along typically conservative-liberal fault lines in the body

[39] *See* Defense Production Act of 1950, Public Laws–Chs. 923, 924, 932, Sept. 8, 1950, p. 798, H.R. 9176, Pub. L. 81–774

[40] For example in parastatal organizations.

politic and the lobbyists would do their part to influence the debate.

2.5.3 Voluntary Code of Conduct

In the absence of this possibility, the enforcement of Security Council resolutions and recommendations by the private cyber sector in the U.S. might be carried out based on a type of voluntary industry Code of Conduct. What this means in a practical sense is that the voluntary nature of such a Code would ensure that private enterprise has a type of veto power over the enforcement power of the Security Council. This leads to a type of absurdity that would disable an important power of the United Nations. In effect, it would leave governance of cyberspace to a group of semi-organized un-elected persons who are bound by their fiduciary responsibility to protect the economic interests of their shareholders, and are not legally required to sacrifice those interests for the purpose of international comity or society as a whole.

The solution to this problem is to increase the level of public-private partnership between the Security Council and the multinational cyber enterprise sector. In the same way that private sector advisory groups give guidance and crucial information to law-makers in the Congress of the United States,[41] the United Nations can put in place an advisory system that will enable private enterprise to inform the Security Council regarding the practical steps that might be taken to mitigate a cyber emergency. If there was agreement between the private sector advisory group and the Security Council, then there would be less of a problem at the national level compelling the subsidiaries of the multinationals to carry out the recommendations of the Security Council.

At this time[42] there is no such a collaborative and advisory system in place to inform the Security Council of the concerns and possibilities of action involving the private sector in cyberspace. *This is an institutional weakness in the international system.*

It should be noted that in the majority of nation States, the private sector is not so independent of government policy. It most nations, it would be

[41] So-called "lobby" activity is protected by the U.S. Constitution which has a clause guaranteeing the "right of the people to petition the government". It is found in the First Amendment. Congress may not abridge "the right of the people . . . to petition the Government for a redress of grievances".

[42] July of 2019

impossible or at best detrimental for the private sector to resist the directives of their home governments. In addition, it would be problematical for subsidiaries of foreign multinational enterprises operating in the provisioning of cyberspace services to resist the directives of a host country government. This problem would not be so difficult, except for the fact that the headquarters for the vast bulk of cyberspace is located in the United States, where business has considerable political power in comparison to the government.

2.5.4 Cyber Embargo

The effect of a "cyber embargo" or "cyber blockade" on a nation State would be impressive. For example, if we assume there was no agreement that the government of one belligerent was responsible for launching the cyber attacks that have led to the cyber emergency, yet during public debates in the Security Council it refuses to acknowledge responsibility but instead blames the event on vigilantes or criminal elements, then the mere *threat* of a cyber-blockade should serve as a strong motivator for that government to take strong action *within its own jurisdiction* so as to quash the parties responsible for the cyber emergency. If it is the case that the government actually is responsible for the cyber attacks, but has relied upon private sector vigilantes to carry out its aggressive policy, then the threat of a cyber-blockade likely will compel the offending government to serve up to justice the malicious actors under the pretense that they are the "independent" parties responsible for the cyber attacks.[43] But regardless of the subterfuge, if the level of cyber disturbance is decreased, then the Security Council will have accomplished its objectives.

[43]In the veiled and deceitful world of international diplomacy, it would be possible for a member State to go so far as to take convicted murders away from death row and serve them up as members of a vigilante cyber band. This would accomplish several goals: (a) it would "save face" in the international community so as to keep a patina of innocence for the belligerent government; (b) it would satisfy external observers that the recommendations of the Security Council were being carried out in "good faith"; (c) it might provide the death row inmates with a chance of avoiding their sentence should they continue to cooperate in the charade. The substitution of one person for another in manipulation of perception in international affairs is commonplace during times of national emergency.

2.5.5 Cyber Force as Armed Force

There is an anomaly in Article 41 because it specifies that the measures taken must of a nature "not involving the use of armed force". However, in leading cyber powers, both offensive and defensive cyber weapons are being developed primarily by the military establishment. For example, in the United States, the national defense work in cyber is being pursued by U.S. Cyber Command, formed initially from the U.S. National Security Agency (NSA). It follows that an important part of U.S. response in cyberspace in conjunction with Article 41 measures would be taken by the defense establishment. Since this is a part of the "armed forces", some might interpret this to be prohibited by the limiting language of Article 41. But a literal reading of Article 41 says that the actions taken must not involve use of "armed force". It does *not* say that no action taken may be initiated by the armed forces of a nation. After all, it often is the case that armed forces are used for performing peaceful missions without kinetic fighting. In the case of offensive cyberspace activities conducted by the armed forces of a member State, in accordance with an adopted resolution under Article 41 of the Charter, these should be considered to be military actions "not involving the use of armed force".[44]

2.5.6 CERT Coordination

This type of event is *terra incognita*. Article 41 does not specify the order or sequence of member State support for the measures to be taken. It also does not require that all member States take the same type of action. The coordinated response of multiple member States to a request for a cyber embargo has never been tested. The international community is completely unprepared to conduct this type of operation, even if there were support from the Security Council. At best we could expect a semi-coordinated response similar to how CERT organizations correspond with one another when there is a major malware incident. In the case of a global cyber emergency, the

[44] A single letter makes the difference—"not involving the use of armed force" *c.f.* "not involving the use of armed force*s*". If the language of Article 41 read "forces" (plural form), then it would prohibit cyber defense activities of the US Cyber Command and its equivalent in other member States. (Note: This needs to be checked in different language versions of the UN Charter.)

CERT operations around the world already would be on a state of high alert. Each of these organizations has close connections with the Internet service providers within their jurisdiction. There already is in place a sophisticated system of blocking spam, and containment of cyber malware. Presumably it would be possible to block the IP addresses for entire countries or parts of targeted countries. Such blockage likely would ride upon the pre-existing blocking infrastructure already in place, providing there was cooperation between the groups controlling the crucial transit points of the Internet.[45] The Internet Corporation for Assigned Names and Numbers (ICANN) and Internet Engineering Task Force (IETF) would play a crucial role in coordination of activities to build the methodology for a cyber-blockade that could be put into effect in response to a cyber emergency. This is an extremely diverse groups of stakeholders with no central point of control either organizationally, nationally, or legally. Consequently, we can expect it would be challenging to work out these procedures. The Internet Governance Forum (IGF), an activity supported by the Secretariat of the United Nations might serve as one of the initial institutions hosting discussions on how to build these capabilities for the international cyber stability community of interest and policy making.

Initially, the Security Council operates by leveraging the actions of cooperating member States. Under almost all circumstances, in the event the threat to international peace and security in cyber space originates in non-State organizations, responsibility for taking action would vest in member States and not arise within the peacekeeping machinery of Chapter VII of the Charter. If, however, the disturbance of global cyberspace was of great enough magnitude, then the Security Council might be seized of the matter. There is nothing in Article 41 that limits the actions of the Security Council to be focused solely against nation States. Security Council action can take place against *any* source of instability in global cyberspace, particularly if the source can be identified with reasonable certainty. This would be done

[45] At the top level, "Tier 1" networks operated by large telecommunications providers link together very high speed networks. 'Tier 2" and lower level networks provide their services by purchasing service from the Tier 1 companies. Internet Exchange Points (IEPs) link these larger networks to multiple Internet service providers. In addition, there are a number of sub-networks that perform specialized functions, such as support of specialized research institutions. Individual in-house networks also operate and assign their own addresses (but not domain names). This arrangement is becoming further complicated by the emergence of the Internet of Things (IoT).

through a Security Council resolution calling on member States to take specific actions in support of its objectives. For example, it might call upon member States to increase cooperation between their national security and law enforcement organizations so as to combat the menace of a transnational threat. It might call on member States to ensure that within their territories, at the technical level of management of the Internet, they work to ensure there is a coherence in strategy and perhaps an accounting back to the Security Council of what steps are underway addressing the threat.

In sum, the Security Council has the power to take action not only against an aggressor nation, but against transnational non-governmental actors that threaten the international peace and security of cyberspace.

2.6 Article 42—The Security Council Mobilizes a "UN Cyber Force"

If calling upon resources of member States to address cyber instability is not effective, then the United Nations Security Council has been granted the power to take action on its own accord. Article 42 provides that:

> Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to *maintain* or *restore* international peace and security. Such action may include *demonstrations, blockade*, and other operations by *air, sea, or land forces* of Members of the United Nations.

Even *without* previous actions having failed, it is clear from the language of Article 42 that the Security Council has the option to jump directly into action. It needs merely to "consider" that lesser action would be ineffective. It is true that the United Nations is not a "world government". When set up, it was not designed to have its own military forces. Nevertheless, Article 42 envisages that the United Nations may utilize the "air, sea, or land forces *of Members* of the United Nations".

There has been a significant amount of debate regarding the bleed-through of the barrier between "kinetic" and "cybernetic" conflict. Much of this work

has turned upon the legal definition of warfare, at least in the conventional sense. However, as can be seen from a careful reading of the United Nations Charter, this bleed-through already is written in because of the insertion of "definition-expansion" words such as "other operation". The word "other" has no clear bounded definition.

2.6.1 Blockade

Consequently, a question arises as to whether the use of "cyber force" would be included within the boundary of Article 42. In terms of "blockade" the traditional meaning of the term is the use of land or naval forces to cut off flow of critical supplies to the offending State. This is a 20th Century version of a medieval siege in which a city was surrounded and its supplies of food cut off until its people surrendered.[46] What would be the equivalent in the world of cyberspace? First of all, the wording "demonstration" and "blockade" does not limit the action to kinetic military force. Here a "blockade" would mean the interruption of social media, email, cloud, and other Internet based services. A "cyber blockade". Generally, a blockade does not involve the taking of military action *within* the State being placed under pressure. In cyberspace terms, this would mean that all terminating points of data communications traffic connecting into the offending State would be filtered out. This blockage could be complete or partial; general or specific according to application.

2.6.2 Other Operations

The Charter's language "other operations" and its linkage with "air, sea or land forces" clearly envisages military conflict. The nature of military conflict is that it does not stop automatically at the border of the offending State. What this means in practical terms for cyberspace operations is that the armed forces and their cyber-fighting components are empowered through Article 42 to take actions *within* the nationally sovereign information

[46]Or even before: *See* Titus Flavius Josephus, The Jewish War, trans. H. St. J. Thackeray, Harvard U. Press, Cambridge, 1928, Book 5, p. 41, "The city was fortified by three walls except where it was enclosed by impassable ravines, a single rampart there sufficing." (describing Jerusalem)

space of the offending State. Consequently, the forces operating on behalf of the Security Council would be empowered to penetrate the firewalls and other information security barriers of the targeted State and carry out offensive cyber operations for the purpose of stopping its activities that are a source of instability to global cyberspace.[47] The wording of Article 42 also makes it clear that the Security Council is empowered to launch *kinetic* attacks against computer centers, Internet switching centers, and the internal telecommunications network within the offending State. The Security Council is empowered to conduct cyber warfare, but within the context of Article 42, these actions if taken would be termed "Cyber Peacekeeping".

2.6.3 Demonstration

An additional element of consideration is the concept of "demonstration". In the kinetic world, this refers to showing force. What would this mean in cyber terms? One possible demonstration would be the *temporary* disruption of cyber services for a short period of time, such as 4, 8, is 12 or 24 hours. This might serve as a warning to the offending State regarding the determination of the international community to persist in imposing even stricter controls if cyber stability is not reestablished.[48]

Although this type of scenario is interesting and even fanciful to discuss, its likelihood is very low because of all the preliminary layers of action available for the Security Council to take before reaching the level of urgency required to trigger Article 42. Hopefully the level of urgency generated by a global cyber emergency would never reach a level of concern so as to compel the type of coordination actions envisaged under Article 42.

2.7 How would a United Nations Cyber Peacekeeping Force Operate?

Is there an analogy between the "blue helmet" peacekeeping forces of the United Nations and its equivalent in cyberspace? In the traditional peace-

[47] including downstream kinetic effects

[48] This type of scenario is difficult discuss without approaching the border between scholarship and science fiction.

keeping role for the United Nations, these forces are interposed between belligerents in order to prevent outbreak of hostilities. The object is to keep the situation stable until the Good Offices of the Secretary General or other negotiations are able to work out an agreement to resolve or mitigate the situation that is the source of the violence.[49] Peacekeeping comes into play when first there is an outbreak of violence, and then by one means or another, the United Nations manages to get agreement from both sides to interject forces that will act as a "trip wire" to prevent further escalation and violence.

What would be the equivalent in cyber space where neither governments or the United Nations have exclusive control over the Internet? It is the private sector that operates and owns most of the Internet and its universe of services. Yet given this multi-layered ownership structure of cyberspace, can there by a United Nations Cyber Peacekeeping force? If so, then how would it work? For example, how would United Nations policy as determined by the Security Council be coordinated in a way that would seamlessly recruit the cooperation of the private sector?

2.7.1 The Emergence of Public-Private Partnerships in the United Nations

Public-private partnerships are not new. The creation of partnerships between the United Nations and private enterprise arose as part of the trend towards a multi-stakeholder approach. Consequently, any effort to establish cooperation between the United Nations and the private sector in the realm of cyberspace must be seen within the context of the historical emergence of the multi-stakeholder model of governance. The multi-stakeholder approach for tackling international public policy issues is not something that was forced upon the United Nations. Instead, it was the United Nations itself that invented it. The United Nations recognized the promise of this new model, and acted. Consequently, we can say that multi-stakeholder-ism at its core

[49]Some have argued that United Nations peacekeeping has never actually solved military conflicts but instead has merely acted to make the conflict continue indefinitely and never reach a resolution. *See* Edward Luttwak, Presentation, "How war can bring peace", Creative Innovation conference, Melbourne, 2012 at `https://youtu.be/XTTruD9WTvc` In this line of thinking, instead of allowing the natural process of war to play out and reach its goal, which is to burn out the desire for war between the parties, instead the interposition of peacekeeping forces tends to congeal war so that it never ends.

is "true blue". How did this come about?

By the time of the 55th session of the General Assembly (2001), the idea of "global partnerships" had emerged.

> "[E]fforts to meet the challenges of globalization could benefit from enhanced *cooperation* between the United Nations and *all relevant partners*, in particular the private sector, in order to ensure that globalization becomes a positive force for all." (emphasis added)[50]

The following year (2002) the General Assembly emphasized "developing partnerships through the provision of great opportunities to the private sector, non-governmental organizations and civil society in general".[51]

There was a learning curve for the United Nations. In 2003 it was "still learning how best to utilize the potential benefits of partnerships [and there were] [e]fforts . . . to scale up promising approaches and to learn from experience".[52] Yet, by the 56th session, the United Nations Millennium Declaration[53] was referenced and the definition of external partners continued to expand.[54] This phase of partnerships was an exploratory one, and by the 58th session (2004), some mention was made of "adher[ing] to a common and systematic approach to partnership . . . *without imposing undue rigidity* in partnership agreements".[55] There also was a reminder that "voluntary partnerships . . . are . . . not intended to substitute for the commitments made by Governments"[56] and much emphasis was placed on the "exchange of . . . information [between the partnerships and] Governments [and] other

[50]Resolution adopted by the General Assembly, Towards global partnerships, 6 March 2001, A/RES/55/215, para. 4.

[51]*See* General Assembly A/RES/56/76 of 24 January 2002

[52]Report of the Secretary-General, Enhanced cooperation between the United Nations and all relevant partners, in particular the private sector, 18 August 2003, A/58/227.

[53]*See* A/RES/55/2

[54]*See* "[D]eveloping partnerships through the provision of greater opportunities to the *private sector*, *non-governmental organizations* and *civil society* in general so as to enable them to contribute to the realization of the goals and programmes of the Organization" (emphasis added), A/RES/56/76, para. 5

[55]Towards global partnerships, A/RES/58/129, numbered paragraph 2 (emphasis added)

[56]*Ibid*, numbered paragraph 5

stakeholders".[57] These resolutions would indicate that there had been perhaps complaints about rigidity, lack of sufficient exchange of information and reporting, and ambiguity regarding the role of governments when one of these new forms of partnership were put in place.

It is clear that the United Nations was going through an adjustment phase. The multi-stakeholder approach was new, and there were inevitable bugs that had to be worked out. Nevertheless, it was recognized that "partnerships are an integral part of the work of much of the United Nations system".[58] By 2005, it was recognized that the United Nations needed to change its own operations to accommodate this new approach including "increasing institutional capacity in country offices, . . . training of staff, [and] streamlining . . . [of] guidelines".[59] By 2007, it was able to say that "since the 1990s, the private sector and other stakeholders have increasingly become active partners in helping the Organization achieve its goals, as a complement to Government action."[60] The multi-stakeholder approach was being used in a variety of ways including training and sharing of best practices. Nevertheless, there was a recognition that the United Nations was compelled to assess its own institutional capacity for effective partnering. In addition, much thought had to be put into the legal relationship between the United Nations and external partners, particularly as regards contracts and liability.

> "Nothing in such a partnership shall be deemed to establish either party as the agent of the other party or create a 'legal' partnership or joint venture between the parties. Neither party has power to bind the other party or to contract in the name of the other party or create a liability against the other in any manner whatsoever".[61]

In its relationship with the business sector, the United Nations set up a

[57] *Ibid*, numbered paragraph 8

[58] *See* Report of the Secretary-General, Enhanced cooperation between the United Nations and all relevant partners, in particular the private sector, 10 August 2005, A/60/214.

[59] *Ibid*, A/60/214

[60] *See* Report of the Secretary-General, Enhanced cooperation between the United Nations and all relevant partners, in particular the private sector, 14 September 2007, A/62/341.

[61] United Nations, Guidelines on Cooperation between the United Nations and the Business Sector, 20 November 2009, para. II.6

number of "internal and external information sharing platforms" to exchange information. For the management or even monitoring of cyberspace necessary for peacekeeping operations, these information sharing arrangements have not been as well developed as they would need to be.

It is important to keep in mind, however, that the concept of multi-stakeholder-ism has nothing to do with actual control over setting of international public policy. There is nothing in any United Nations document that suggests even in the most remote sense that anyone other than governments will set policy. The sharing of information, and the joint conducting of activities between the United Nations and businesses, or Non-Governmental Organizations (NGOs) or others, is designed to carry out the policies that have been set by the General Assembly or in some cases the Security Council. In other words, multi-stakeholder-ism was designed to assist the United Nations in carrying out its objectives, but it was not designed to change in any way the multilateral nature of the institution, and the same model has been propagated to subsidiary parts of the United Nations system such as the World Health Organization (WHO), the International Civil Aviation Organization (ICAO), and essentially to all subsidiary UN bodies.

There is, nevertheless, a widely-held notion that these partners of the United Nations can do very much to influence public policy setting. Throughout the United Nations system, these partners provide advice, identify key issues, give options for possible policies, make suggestions for improvements, and in general support policy-making, and this incoming information is widely considered to be vital. Nevertheless, when it comes to actually setting the policy, it is the nation states that do it. Member states of the United Nations listen to everyone, but they make their own decisions.

So the role of the private sector in helping carry out the resolutions of the Security Council would sit solidly within the evolving multi-stakeholder efforts of the United Nations, but we can also see that these efforts themselves are not static or sufficiently defined and consequently would represent a learning curve for everyone involved. One lingering question, however, is whether the private sector community managing cyberspace can increase its activities in providing insights or advice for global cyber stability.

2.7.2 Public-Private Partnerships and a UN Cyber Force for Peacekeeping

In the same way that the United Nations does not possess a military force, it does not possess a cyber force. Consequently, in order to make cyber peacekeeping work, it would be necessary for those private sector and government-based cyber monitors involved in peacekeeping to provide a stream of regular reporting of their information to a United Nations based cyber operation. There is no such operation within the United Nations and in order to carry out cyber peacekeeping, it would need to be configured. One complimentary aspect of cyber peacekeeping is that since it involves the use of *virtual* force, the operational costs of such action likely would be far less than that associated with the deployment of "boots on the ground" under the older form of peacekeeping.

Currently[62] the United Nations is operating thirteen peacekeeping missions using more than 80,000 military, police, and civilian personnel. The United States pays for 27.9 percent of the cost.[63] The UN peacekeeping budget is 6,510 million USD per year. South Sudan takes 1,180 million per year. Congo takes another 1,010 million per year.

At a minimum there would be cost in providing a unified systems application interface that could be monitored by a staff that then could report its results to the authorities within the United Nations. This appears well within the means of the United Nations.

Does this mean that the Security Council would be able to "fight" a cyber conflict? It depends on the definition of "fighting". That in turn depends on the level of effective coordination between the underlying groups controlling the Internet and the Security Council. How would this work?

See Table 3 on Page 50. Levels of coordination needed for the Security Council to be able to effectively engage in cyber peacekeeping. In many nations, including the United States, there is no legal framework in place to compel this type of coordination. Consequently, it is an open issue how this type of peacekeeping would work. It is certain that public opinion would play a crucial role in building consensus.

[62] Spring of 2020

[63] China pays for 15 percent.

The deployment of a United Nations Cyber Force for Peacekeeping presupposes it is possible to identify the belligerents, and then it is possible to get agreement for a role of the United Nations in keeping the peace. But the physical implementation of these measures would be completely different. In the case of a kinetic "ground" conflict, there is a definable physical border than can be specified in order to locate and define a base of operations for the United Nations peacekeeping forces. There is no such border in cyberspace. Nevertheless, even though it is not possible to define a *physical* border, it would be possible to define a *logical* border within cyberspace. *It would be here that the United Nations would place its peacekeeping forces.* In practical terms, this would imply that telecommunications operators, social media providers, cloud services and other Internet-based applications providers would act to monitor the flow of cyber space communications so as to ensure that no aggressive cyber attack traverses the logical boundary separating the belligerents. This would imply that in order for the Security Council to put in place a cyber peacekeeping force, it would be necessary to get an agreement from the belligerents that any Internet traffic flowing from one to another would be monitored so as to ensure that it did not contain malware or untoward machine instructions.

This would be equivalent to placing a nation on an enhanced "watch list" in which the Internet communications originating on its territory would be subject to enhanced scrutiny and even temporary waylaying or cyber quarantine until such time as it was determined that the content was harmless. This would be an initial step that could be taken before there was an effort to actually severe telecommunications services or access to applications. This imposition of a "cyber quarantine" would serve as a type of warning to the offending nation that more stringent steps could be taken later unless its behavior is improved.

The use of data mining and profiling through social media would allow the Security Council to engage in the equivalent of "precision cyber bombing". If the same type of algorithms were used for targeting of offending groups as are used in the provisioning of online advertising, then it would be possible for the Security Council to target via the same cyber tools very specific sub-groups of persons. It would be possible, for example, to temporarily suspend the Internet activities of all men in a country if there were widespread harassment or persecution of women. It would be possible to turn off Internet services for only certain cities, or neighborhoods associated with where government

workers live. It would be possible to target universities or scientific research establishments, or the government or military sectors without harming or interrupting the Internet activities of others within the society. It would be possible to interfere with the information operations of one political party while leaving other untouched. See Table 2 on Page 49.

Cyber is an extremely powerful weapon that can be put into play during a social disturbance. For example, in the midst of a social revolution within a country, it would be possible to disable the government but allow the social media services of the dissidents and revolutionary forces to continue their operations without interruption.[64] This type of intervention into the social dynamics of a country would be extremely significant.[65]

The practical implication of this flexibility in targeting of cyber sanctions is that *the effective power of the Security Council has been significantly increased in comparison to what traditionally has been possible using conventional military force.* It also implies that the peacekeeping operation within the Security Council would be given access to real-time reporting of any cyber events flowing between the belligerents.

[64](or the other way around)

[65]An example of the dynamics in such a situation would be the role of social media during the Arab Spring when the Internet was used as a powerful organizing tool for dissidents seeking to overthrow the government.

OSI Level	Effect on Telecommunications and Social Media
End-User Applications	Apps on devices of citizens; this could be highly if appropriate data-mining and profiling were used
Cloud Services and Enterprise Applications	Shared application delivery platforms provided from overseas locations for service within the offending state; In-country cloud operations of foreign providers of services willing to comply with Security Council resolutions
Telephone and Telegraph termination and switching	Blockage of central switch signalling mechanisms linking the telephone network of the offending country through International Record Carriers; this may also terminate all data communications regardless of the content of the data streams
Satellite and Wireless	Other underlying infrastructure providers would turn off access in to and out of the offending country

Table 2: Relationship between the International Organization for Standardization (ISO) Interconnection model and the imposition of United Nations sanctions through the Security Council.

Coordination Level	Operational Power and Scope
Security Council	Responsible for setting overall strategic direction of the peacekeeping and cyber stability actions to be taken by member States
Member States Cyber Defense Operations	Responsible for monitoring activities of the government of the offending member State; center for coordination of other actions within its national sovereignty including interface with International record carriers and Service Providers
International Record Carriers	Management and reporting on data communications traffic traversing the border of the offending state; power to terminate or block services
Computer Emergency Response Teams (CERT)	Power to verify the existence of malware and forensic analysis to verify the source or "signature" on malware; exchange of information regarding the cyber exploits and vulnerabilities being used by cyber combatants so as to accelerate the interposition of defensive cyber measures with a view to mitigating the level of cyber destruction
Internet Service Providers	Supplementary power to blockade or interrupt services in the offending State; possible use of deep packet inspection to ensure compliance with Security Council resolutions; possible operation of quarantine of data for safety certification; reporting of data to Security Council or national authorities
Application Service Providers	Power to cut off services such as social media, email, and database access; power to use big data mining and advertising algorithms to selectively target groups within the offending State; possible real-time reporting of activity and signals intelligence (SIGINT) to national authorities

Table 3: UN Cyber Force for Peacekeeping