CYBER WARFARE AND THE CRIME OF AGGRESSION: THE NEED FOR INDIVIDUAL ACCOUNTABILITY ON TOMORROW'S BATTLEFIELD

JONATHAN A. OPHARDT[1]

ABSTRACT

As cyberspace matures, the international system faces a new challenge in confronting the use of force. Non-State actors continue to grow in importance, gaining the skill and the expertise necessary to wage asymmetric warfare using non-traditional weaponry that can create devastating real-world consequences. The international legal system must adapt to this battleground and provide workable mechanisms to hold aggressive actors accountable for their actions. The International Criminal Court—the only criminal tribunal in the world with global reach—holds significant promise in addressing this threat. The Assembly of State Parties should construct the definition of aggression to include these emerging challenges. By structuring the definition to confront the challenges of cyberspace—specifically non-State actors, the disaggregation of warfare, and new conceptions of territoriality—the International Criminal Court can become a viable framework of accountability for the wars of the twenty-first century.

INTRODUCTION

¶1 Cyber warfare, a subset of a larger field known as information operations,[2] until recently appeared to belong to the realm of science fiction. Although cyber attacks have occurred throughout most of the Internet's history,[3] States have just begun to include them in their doctrine

---

[1] A.B. 2003, Princeton University; J.D. Candidate 2010, Duke University School of Law; former Electronic Warfare Officer, United States Air Force. A special thanks to Professor Noah Weisbord for all his assistance and patience. All views and opinions expressed in this iBrief are those of the author alone and do not reflect those of any other individual, the Department of Defense, the United States Air Force, or any other government agency.

[2] THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 29 (2000).

[3] *Id.* at 23.

and tactics.[4] Cyber attacks do not fit neatly into the traditional international framework governing the use of force. Cyber attacks represent a new form of disaggregated warfare, substantially conducted by non-State collectives, that displays new conceptions of territoriality. These challenges require substantial adjustments of the international system. The Assembly of State Parties' (ASP) on-going effort to define aggression presents a powerful opportunity to confront both of these issues simultaneously. The ASP should adapt its definition to better account for this emerging threat by including the aggressive acts of non-State collectives. That definition should be broadly interpreted by the International Criminal Court (ICC) to include these new conceptions of territoriality and, most importantly, the new weapons of cyberspace.

I. NOTABLE INSTANCES OF CYBER ATTACK – THE NEW BATTLEFIELD OF CYBERSPACE

¶2 Just before midnight on August 8, 2008, Georgian military personnel moved into the semi-autonomous region of South Ossetia.[5] Georgia maintains its military action was purely responsive to Russian conduct.[6] Georgia cites both steadily increasing attacks from separatist groups and alleged incursions by Russian troops into South Ossetian territory as justification for their subsequent armed response.[7] Russia continues to claim that it acted only after Georgia made a brash attempt to reclaim its break-away providence.[8]

¶3 The bombs and bullets flew simultaneously with packets and botnets. For the first time, a ground attack coincided with a cyber attack.[9] Georgian websites were bombarded by thousands of computers in what technology experts call a Distributed Denial of Service attack, or DDoS.[10]

¶4 Denial of Service (DoS) attacks can be accomplished with only one computer, and in a multitude of ways. The goal of a DoS attack is to prevent

---

[4] John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at A1, *available at* http://www.nytimes.com/2008/08/13/technology/13cyber.html.

[5] GOVERNMENT OF GEORGIA, CHRONOLOGY RUSSIAN AGGRESSION IN GEORGIA 13 (June 19, 2009), http://georgiaupdate.gov.ge/en/doc/10010584/CHRONOLOGY%20MIA%202020 08.pdf.

[6] *Id.*

[7] *Id.*

[8] Anne Barnard, *Russians Push Past Separatist Region, Assaulting a City in Central Georgia*, N.Y. TIMES, August 11, 2008, at A1, *available at* http://www.nytimes.com/2008/08/11/world/europe/11georgia.html.

[9] Markoff, *supra* note 4.

[10] *Id.*

the intended individual users from utilizing a certain networked resource. A variety of techniques are available to exploit the underlying Internet communication architecture and prevent legitimate use of networks. Most DoS attacks flood the target network with bogus traffic or overwhelm a target computer with bogus requests preventing the legitimate use of either resource.

¶5 DoS attacks evolved to DDoS attacks, which are much more debilitating and considerably more difficult to defend against. DDoS attacks use primarily the same tactics as a DoS attack but from multiple source computers. These computers are usually controlled remotely through vulnerabilities or previous malware infections. Vulnerability attacks exploit existing deficiencies in the operating software of a computer. These 'bugs' can be used to either disable the targeted computer, or in some instances can be used to cause the targeted computer to attack a second computer, without the knowledge of the targeted computer's owner.[11] More commonly, DDoS attacks utilize malicious software (or malware). Malware refers to computer code specifically written with harmful intent.

¶6 The false requests from a DDoS attack caused Georgian government websites to go offline.[12] Internet service in Georgia slowed to a crawl as bogus requests clogged the limited data routes in and out of the country.[13] Georgian government officials experienced extreme difficulty communicating with their citizens and the outside world.[14] Hackers defaced Georgian websites with Russian nationalistic propaganda.[15] Georgia blamed the Russian government, claiming it was the victims of State cyber warfare.[16] Russia denied sponsoring or supporting any cyber attack on Georgia.[17] Russian officials claimed the attacks were likely the result of overzealous individuals acting on nationalistic sentiment.[18]

A new form of warfare

¶7 When considering the impact of cyberspace on international law, it is important to note the differences between the variable levels of malicious cyber activity, which include cyber crime, cyber espionage, cyber terrorism,

---

[11] *See* DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 234–37 (1999) (explaining various tactics used to exploit existing weaknesses in server management software, specifically a UDP packet storm where target computers are used to disable each other).
[12] Markoff, *supra* note 4.
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] Markoff, *supra* note 4.
[18] *Id.*

cyber attacks, and cyber warfare.[19] The intentions of the perpetrator and the effects of the act are one useful way to classify the malicious activity.[20] Cyber crime is activity conducted for profit, primarily motivated by financial gain or notoriety.[21] Cyber crime typically involves the production of malware, the distribution of child pornography, hijacking for ransom, the sale of mercenary services, and the like.[22] Cyber espionage is characterized by a motivation to discover sensitive information rather than that of causing harm.[23] Cyber espionage can be conducted by an individual or a collective with the goal of pecuniary gain or strategic military advantage.[24] Cyber terrorism, like all terrorism, is intended to influence an audience or motivate a government through threats and violence.[25] Cyber terrorists use the malicious tools available in cyberspace as weapons against cyber and real world targets.[26]

¶8 The definition of cyber attack remains inconsistent. Some commentators use the term to encompass a wide variety of acts of cyber terrorism and cyber warfare.[27] Other commentators use cyber attacks as a separate category.[28] Even among these experts, usage varies. Some argue that cyber warfare requires the simultaneous use of conventional weaponry.[29] Others categorize cyber attacks by the identity and motivations of the attackers.[30] Still others look to the type of targets and degree of harm caused by the attacks.[31] No expert questions that Georgia was the victim of organized cyber attacks, but many experts scoff at the notion that the attacks amounted to cyber warfare.[32]

¶9 One difficulty in the treatment of cyber attack in international law stems from the ease with which an attack can morph between levels, and the

---

[19] *Technology Quarterly-Cyber Warfare: Marching Off to Cyberwar*, THE ECONOMIST, Dec. 6, 2008, at 71, *available at* 2008 WLNR 23421990 [hereinafter ECONOMIST].
[20] Solce, *The Battlefield of Cyberspace: The Inevitable New Military Branch - The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 301 (2008).
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] Solce, *supra* note 20.
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] ECONOMIST, *supra* note 19.
[30] *Id.*
[31] *Id.*
[32] Ethan Zuckerman, *Misunderstanding Cyberwar in Georgia*, REUTERS, Aug. 16, 2008, http://www.reuters.com/article/reutersEdge/idUSGOR66065320080816.

difficulty in determining the level at the time of the attack. The steps used to gain access to a network for the purposes of espionage will be nearly identical to those used for access in wartime. While disguise and deception have been a part of warfare since ancient times, the ease and speed with which a cyber infiltrator can change roles coupled with the potential devastation from an attack on certain networks create a need for swift defensive actions. Due to these difficulties, a cautious network defense may treat lower level attacks and more serious attacks similarly. These challenges create a significant proportionality issue in self-defense decisions.

¶10 While the cyber attacks launched to date may seem relatively tame when compared to the destruction capable of traditional instrumentalities of war, experts generally agree that potential cyber attacks of the very near future are likely to carry significantly greater consequences.[33] The greater the network integration of a target country's infrastructure, the greater its potential vulnerability.[34] Georgia and Estonia suffered limited real world consequences from their attacks largely due to their limited reliance on cybernetic networks.[35] In a country as reliant as the United States, hypothetical targets include the disabling of water purification systems,[36] the intentional misrouting of trains causing massive collisions,[37] the disruption of air-traffic control,[38] the intentional opening of dams,[39] and

---

[33] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 894 (1999); Roger W. Barnett, *A Different Kettle of Fish: Computer Network Attack, in* 76 INTERNATIONAL LAW STUDIES, COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 21, 31–32 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002).

[34] *Id.*

[35] ECONOMIST, *supra* note 19. It is important to note, however, that Georgia and Estonia were both more susceptible to DDoS attacks due to their relatively small internet accessibility. Internet traffic is designed to take the fastest route to its destination, not the geographically shortest. When a network has relatively few nodes through which to route packets of information, slowing or clogging them with a DDoS attack is relatively easy. Such a country-wide DDoS attack would be extremely challenging in the United States, as packets would automatically route around the slow nodes. So while increased reliance and interconnectivity can result in greater significance of attack, it also increases the difficulty of rendering wide-spread service outages through the DDoS methods used against Georgia.

[36] David Tubbs, et al., *Technology and Law: The Evolution of Digital Warfare*, *in* INTERNATIONAL LAW STUDIES, COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 33, at 7, 18.

[37] ECONOMIST, *supra* note 19.

[38] *Id.*

[39] *Id.*

potentially the meltdown of nuclear reactors,[40] all resulting in significant loss of life and property very much on par with damage caused by traditional weaponry.[41]

¶11 Actual loss of life and destruction of property are possibilities of cyber attack, but the more likely and prevalent threat stems from malicious interference with communication networks and economic markets. A cyber attacker could manipulate the stock market or cause massive and sustained outages of wireless networks.[42] While these acts lack the physical destruction of other attacks, the potential economic consequences and breadth of their impact make them a serious threat to the security of a State. When the greater likelihood of these attacks is combined with the possibility of sustained or repeated interference with these increasingly important aspects of our infrastructure, the threat seems quite ominous. However, even a State-sponsored manipulation of economic markets would fail to meet the traditional definition of international aggression.[43]

Substantial Involvement of Non-State Actors

¶12 The current State actor requirement in international law greatly limits its applicability to cyber attacks. Evidence certainly shows that a portion of the attacks on Georgia were carried out by individuals without direct affiliation to any group or State.[44] Websites displayed how-to guides providing eager individuals step-by-step instructions on how to configure their computers to attack Georgian websites.[45] Other websites coordinated the volunteers by posting the statuses of target sites.[46] This information allowed individuals to redirect their computers from disabled targets to new targets.[47] Yet these voluntary attacks gained momentum only after the initial

---

[40] John F. Murphy, *Computer Network Attacks by Terrorists*, *in* INTERNATIONAL LAW STUDIES, COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 33, at 323, 326.

[41] It should be noted these attacks would generally require significantly greater sophistication than that shown in the Russian-Georgian conflict. While the tools are certainly available and the defenses frequently porous enough, how widespread and how porous are issues of strenuous debate.

[42] Solce, *supra* note 20, at 310.

[43] *See* Noah Weisbord**,** *Conceptualizing Aggression*, 20 DUKE J. COMP. & INT'L L. 1, 33 (2009) [hereinafter Weisbord, *Conceptualizing Aggression*], *available at* http://www.law.duke.edu/shell/cite.pl?20+Duke+J.+Comp.+&+Int%27l+L.+1+pdf.

[44] ECONOMIST, *supra* note 19.

[45] *Id.*

[46] *Id.*

[47] *Id.*

wave of cyber attacks.[48] Most importantly, they fail to explain the 'staging attacks', or trial runs, that occurred weeks prior to the ground war.[49]

¶13 In July, independent non-profit monitoring groups noticed a significant number of malicious attacks on Georgian websites.[50] These attacks were debilitating but brief, likely a dress rehearsal for the August attacks.[51] Some of the very same websites attacked in July were attacked again in August after the conventional war began.[52] The immediate coordination and the sophistication of the August attacks suggests strong organizational influence.[53] Many have suggested responsibility for the attacks rests with a nefarious organization, the Russian Business Network (RBN).[54]

¶14 The RBN thrives in the largely unregulated and wild-west atmosphere of Russian cyberspace.[55] The RBN has a hand in some of the worst aspects of the Internet.[56] Child pornography, malware, spam, identity theft, and offensive cyber attack capabilities are sold for profit by the RBN.[57] Although the RBN has no headquarters, website, or legal status, their name appears on the registration of thousands of websites.[58]

¶15 Independent companies are also available for hire to direct cyber attacks at 'legitimate' targets.[59] Sony, Universal and other large copyright holders have hired such independent companies to initiate DDoS attacks against users of file sharing software suspected of sharing their copyrighted materials.[60] However, these cyber-mercenaries are not overly discriminating in their target selection.[61] One reason file sharing software remains legal is its ability to allow lower budget producers to share their work.[62] In the past,

---

[48] Markoff, *supra* note 4.
[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] Markoff, *supra* note 4.
[54] *Id.*
[55] *See* Brian Krebs, *Shadowy Russian Firm Seen as Conduit for Cybercrime*, WASH. POST, Oct. 13, 2007, at A15, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html.
[56] Markoff, *supra* note 4.
[57] *Id.*
[58] Krebs, *supra* note 55.
[59] David Gewirtz, *Digital Defense: The Coming Cyberwar*, 14 J. COUNTERTERRORISM & HOMELAND SECURITY INT'L 3 (2008).
[60] *Id.*
[61] *Id.*
[62] *Id.*

mercenaries have mistakenly targeted these legitimate users.[63] While their inadvertent attacks cause no tangible damage, the economic consequences can be dire.[64]

¶16 Other independent companies have even engaged in repeated cyber attacks against each other. Competition between Internet service providers (ISPs) has led companies to orchestrate DDoS attacks on each others' networks in an attempt to hurt their competitor's quality of service.[65] These non-State 'legitimate' international actors highlight the necessity of transnational cyber attack regulation. They also illustrate the substantial likelihood of actual cyber mercenaries who conduct cyber attacks on behalf of aggressive States. The international legal regime must consider these groups when drafting tools to punish aggressive acts.

¶17 Other individuals face interesting dilemmas in the cyber frontier.[66] "Bug hunters" are private individuals who can make significant incomes discovering the flaws in commercially available programming.[67] They then sell their discoveries to other interested parties.[68] Some of the purchasers are the software writers themselves, others are security firms, and still others are motivated by the pure profit afforded by the secondary black market, or worse their own hacking and malware projects.[69]

¶18 This market for vulnerabilities remains completely unregulated.[70] Some individual bug hunters practice self-regulation by refusing to sell their discoveries to foreign interests.[71] However, the bugs they sell provide keys to the doors through which cyber warfare can be waged.[72] States are known purchasers of bug information, and their interest is likely to grow.[73] As the cyber age expands into the area of warfare, international law must be equipped to regulate the broad diversity of actors who will play important roles in tomorrow's aggressive wars.

---

[63] *Id.*
[64] *Id.*
[65] Denning, *supra* note 11, at 236.
[66] Michael Reilly, *How Long Before All-out Cyberwar?*, NEW SCIENTIST, Feb. 23, 2008, at 24, *available at* http://www.newscientist.com/article/mg19726446.100-how-long-before-allout-cyberwar.html.
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] Reilly, *supra* note 66.
[73] *Id.*

The Disaggregation of Warfare

¶19 International law is ill-equipped to adjust to the disaggregation of warfare made possible by the cyber age. Combatants and assets need not physically gather together to conduct their attack. Each asset is capable of contributing to the collective effort despite physical distance. This is achieved through the global reach of the Internet, and the homogeneity of the software running on the computers that it connects. A bug hunter only gains importance though the remarkable similarities in software design and use around the globe. These similarities create the global market for discovered security flaws, and those flaws are fundamental tools in the writing of malware.

¶20 Some malware allows targeted computers to be 'slaved' to the commands of a single operator who can remotely control aspects of their behavior. These 'slave' computers are commonly known as 'botnets.' Botnets can be instructed to carry out activities of the same character as a DoS attack. However, by their coordinated efforts, these botnets are able to achieve greater devastation than possible from a single machine.[74] DDoS attacks are capable of creating significant effects on entire networks without specifically targeting every computer on the target network.

¶21 The Internet's architecture and homogeneity permits remote, largely anonymous world-wide access, thereby allowing the triggering of botnet attacks from any computer with internet connectivity. These same characteristics also allow the assembly and use of cyber weaponry on a global scale. For example, the RBN controls multiple world-wide botnets, capable of being used for DDoS attacks similar to those used against Georgia.[75] Infected computers scattered across the globe reportedly can be rented for four cents a machine, providing the equipment needed for a

---

[74] It is important to note that botnets are useful in activities other than DDoS attacks. Botnets can be used for other malicious purposes, including spam. For those fortunate enough to not know, spam is the electronic equivalent of junk mail. Spam messages are unsolicited e-mail, generally advertising products or websites. Botnets are used to hide the source of spam so as to avoid the rather extensive filters in use by most e-mail providers, and can be used to execute e-mail floods or bombs.

A form of volunteer botnet has become greatly popular to assist in the examination of scientific data. Called distributive computing, users install software on their computer that allows its hardware to be used to examine data from various scientific experiments. This distributive computing provides a source of free computing power normally requiring extremely expensive supercomputers. For an example, see Gewirtz, *supra* note 59 (discussing Folding@home, which uses distributive computing to conduct studies of protein folding and molecular dynamics).

[75] Krebs, *supra* note 55.

DDoS attack to any paying party for use against any desired target.[76] Alternatively, the RBN could have donated its services in the spirit of nationalistic motivations. Such an unsolicited donation may explain the cyber attacks suffered by Georgia. Botnets allow a cyber attacker to implement a coordinated attack from numerous locations, including within the target network, with very limited warning for a nominal cost. These types of cyber attacks defy the simple categorization of traditional weaponry currently used in international law.

¶22 The cyber attacks on Georgia were not the first instance of coordinated attacks directed at a former Soviet State.[77] Estonia suffered similar DDoS attacks in 2007.[78] Those attacks began following the Estonian government's decision to relocate Soviet era monuments.[79] The attacks targeted government websites and several Estonian banks.[80] Communication with Estonian emergency services was briefly interrupted.[81] The Estonian government blamed the Russian government.[82] The Russian government denied any involvement.[83] An investigation by Estonian authorities resulted in charges against an ethnic Russian living in Estonia for his limited role in the cyber attacks.[84] However, the investigation still continues, and many observers suspect RBN—if not Russian intelligence agency—involvement.[85]

¶23 In general, while tracing an attack is possible, most traces terminate at the ISP. An ISP subscriber may be the responsible party, or the ISP may be yet another conduit through which the attack has been routed. Regardless, further tracing will require ISP cooperation.[86] Estonia's

---

[76] *Id.*
[77] Mark Lander & John Markoff, *First war in cyberspace: The lessons of Estonia*, INT'L HERALD TRIBUNE, May 29, 2007, at 1, *available at* 2007 WLNR 10334241.
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] ECONOMIST, *supra* note 19.
[82] RUSSIAN LIFE, *supra* note 77.
[83] *Id.*
[84] Thomas Claburn, *Estonian Hacker Fined for Cyberattack*, INFORMATIONWEEK, Jan. 25, 2008, *available at* http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=205918839.
[85] *Id.*
[86] Murphy, *supra* note 40, at 327. For an interesting discussion of 'rogue' ISPs and the difficulty in having their connectivity to the internet severed, see Brian Krebs, *A Closer Look at McColo*, WASH. POST, Nov. 13, 2008, *available at* http://voices.washingtonpost.com/securityfix/2008/11/the_badness_that_was_m

difficulties in tracing and prosecution are emblematic of the inherent investigative difficulties caused by the disaggregation of cyber warfare. The number and diversity of culpable individuals involved in international cyber aggression requires an appropriately tailored and flexible definition of aggression.

New Conceptions of Territoriality

¶24 Cyberspace challenges a fundamental aspect of international law—territory. This is best exemplified by the inherent structure of the Internet when applied to a DDoS attack utilizing a botnet. Botnets are not limited geographically; the malware that creates them moves freely across national borders. A DDoS attack using a botnet will cause assets scattered across the globe to attack a target through the Internet. Internet traffic was specifically designed to travel over the fastest route possible.[87] This route is not necessarily the same as the most geographically direct route.

¶25 Information sent over the Internet is divided into packets. These packets adapt their routes to network congestion, moving through nodes that result in the fastest communication. Not every packet in a message will take the same route, as system dynamics change during transmission. After the packets arrive, often at different times, the target computer reassembles them to recreate the message. The result of such a system creates complex, often circuitous routing across substantially more international borders than traditional instrumentalities of warfare.[88] The routing and tracing difficulties create significant challenges for the active defense against attacks and also the law regulating the use of force.[89]

¶26 Cyber attacks are not limited to Russia and its former satellite States.[90] The United States has suffered multiple attacks, allegedly of Chinese origin.[91] These attacks, code named 'Titan Rain,' nearly disrupted power on the West Coast and resulted in multiple security breaches at defense contracting companies.[92] Another suspected Chinese attack

---

ccolo.html (discussing the termination of McColo, a suspected ISP for the RBN which, when disabled, resulted in the significant reduction of worldwide spam).

[87] Tubbs, et al, *supra* note 36, at 10.

[88] *Id.*

[89] Daniel B. Silver, *Computer Network Attack as a Use of Force under Article 2(4), in* INTERNATIONAL LAW STUDIES, COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 33, at 73, 79.

[90] Carolyn Duffy Marsan, *How close is World War 3.0?*, NETWORK WORLD, Aug. 22, 2007, at 1, *available at* http://www.networkworld.com/news/2007/082207-cyberwar.html.

[91] *Id.*

[92] *Id.* at 2.

purportedly disrupted power to fifty million people in North America.[93] These attacks are generally considered probing attacks, designed to test American countermeasures.[94] Britain also has reported cyber attacks from both State-sponsored and terrorist sources, referring to them as "remarkable" in number.[95]

¶27 Not all attacks fit neatly into this traditional attacker/attacked State framework. At the height of the cyber attacks against Georgian websites during the Russia-Georgia conflict, many besieged websites were temporarily moved to servers located in the United States.[96] The attacks continued but the new hosts were better able to defend against them.[97] While the attacked server was located in the United States, the 'territory' in cyberspace being interfered with was that of Georgia.

¶28 Smaller groups and individuals are increasingly capable of cheaply and efficiently creating significant damage in cyberspace that results in real world consequences.[98] Attacks are difficult to trace and current legal structures make prosecution extremely unlikely.[99] As greater reliance on computer networks expands throughout the globe, the potential destruction resulting from these attacks will increase.[100] So, too, will the number of attacks, unless this increase in potential impact is not counterbalanced with an increase in risk to the future perpetrators.[101]

¶29 The international community must recognize this emerging challenge and structure an international response accordingly. Aggression in cyberspace requires an international solution. Cyber attacks lack the traditional geospatial limitations of traditional aggression. The Internet's structure permits attacks to occur from any part of the globe against any target with no early warning or indication. International attempts to regulate

---

[93] Gewirtz, *supra* note 59.
[94] Marsan, *supra* note 90.
[95] Jonathan Richards, *Thousands of Cyber Attacks Each Day on Key Utilities*, TIMES (U.K.), August 23, 2008, at 9, *available at* http://www.timesonline.co.uk/tol/news/uk/crime/article4592677.ece.
[96] Ed Sutherland, *Georgian president relocates website to Atlanta*, ALL HEADLINE NEWS, August 11, 2008, http://www.allheadlinenews.com/articles/7011905889.
[97] *Id.*
[98] Barnett, *supra* note 33, at 26–27.
[99] *See* Claburn, *supra* note 84.
[100] *See* Tubbs et al, *supra* note 36, at 19; Phillip A. Johnson, *Is It Time for a Treaty on Information Warfare*, *in* INTERNATIONAL LAW STUDIES, COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 33, at 439, 441.
[101] *See* Arthur K. Cebrowski, *CNE and CNA in the Network-Centric Battlespace*, *in* INTERNATIONAL LAW STUDIES, COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 33, at 1, 4.

cyber attacks must create *individual* accountability for the malfeasance of State and non-State actors. The crime of aggression and the ICC provide a unique opportunity and appropriate method for tackling this important issue.

II. INDIVIDUAL CRIMINAL RESPONSIBILITY FOR CYBER ATTACKS: THE EMERGING DEFINITION OF THE CRIME OF AGGRESSION

¶30 Contemporary international law prohibits the use of force between States except with UN Security Council authorization or in self-defense.[102] A 1974 General Assembly (GA) Resolution interprets these restrictions with more specificity.[103] The Resolution (1) limits aggression to the use of traditional armed force, (2) is highly State centric, (3) uses examples of traditional aggregated warfare, and (4) relies on traditional concepts of territorial integrity.[104]

¶31 The 1974 GA Resolution is the basis for the emerging definition of the crime of aggression in international criminal law, the front in the larger international law debate over the difference between legal and illegal uses of force.[105] The 1974 GA Resolution served as the foundation in the negotiations to determine which acts of political and military leaders qualify as aggression.[106] As the definition of the international crime of aggression borrows heavily from the 1974 GA Resolution defining an act of aggression, the proposed language has many of the same characteristics.[107]

¶32 The latest SWGCA definition is made up of two core concepts: the State act of aggression and the link between the individual and the State act.[108] The definition of the act of aggression, like the 1974 GA Resolution, limits its applicability to traditional weaponry of warfare, focuses on acts committed by and against States, uses aggregated examples of aggression, and embodies traditional conceptions of territoriality. The link between the individual and the State act is achieved through four components: the leadership clause, conduct verbs, a liability doctrine, and modes of

---

[102] U.N. Charter art. 2, para 4, arts. 39 & 51.
[103] G.A. Res. 3314 (XXIX), U.N. Doc. A/RES/3314 (Dec. 14, 1974) [hereinafter 1974 Resolution].
[104] *Id.*
[105] Noah Weisbord, *Prosecuting Aggression*, 49 HARV. INT'L L. J. 161, 179 (2008) [hereinafter Weisbord, *Prosecuting Aggression*].
[106] *Id.*
[107] ICC, Assembly of States Parties, Special Working Group on the Crime of Aggression, Second Resump. 7th Sess., New York, Feb. 9–13 2009, *Report of the Special Working Group on the Crime of Aggression*, Annex II.Appx.I. ICC-ASP/7/20/Add.1, available at http://www.icc-cpi.int/iccdocs/asp_docs/ICC-ASP-7-20-Add.1-SWGCA%20English.pdf [hereinafter SWGCA 2009 Report].
[108] *See* Weisbord, *Conceptualizing Aggression*, *supra* note 43, at 20.

perpetration/participation.[109] Each choice made by the SWGCA has significant implications for the definition of the crime of aggression when applied to cyber warfare. The 1974 GA Resolution and the SWGCA definition will be examined in relation to the challenges raised by cyber warfare.

A new form of warfare

¶33 The GA Resolution explicitly applies to the traditional instrument of armed force and the traditional weaponry used in armed attacks.[110] Article 3 of the Resolution provides examples of aggression, referring to the attack, invasion, bombardment and blockade of a State by the traditional armed forces—land, air, sea, or marine—of another State.[111] While the Resolution carefully emphasizes that the examples are not exhaustive, power for constituting other acts as aggressive lies solely with the Security Counsel.[112] Indirect force is limited to acts which are sufficiently similar in severity and tactics to be analogous to those of conventional armed forces.[113] Even blockades are only considered aggressive when instituted by the armed forces of another State.[114]

¶34 Armed force was not the only form of force considered by the negotiating States. The 1967 and 1973 Oil Embargoes created significant support for the inclusion of economic aggression in the GA Resolution.[115] The Resolution was purposefully drafted to appease these interests through the inclusion of Article 4, which underscored the exemplary nature of the list.[116] In doing so, the Resolution neither endorsed nor precluded the finding that aggression could take the form of an unarmed act.[117]

¶35 While making a reference to the GA Resolution, the SWGCA included in their proposed definition the Resolution's list of acts from Article 3 that would qualify as aggression.[118] However, they eliminated Article 4, instead agreeing on language that allows for interpretation of the list as either open or closed.[119] By adopting the explicit reliance on traditional instrumentalities and weaponry of Article 3 and eliminating the caveat of Article 4, the SWGCA has severely restricted the application of

---

[109] *Id.*
[110] *Id.*
[111] 1974 Resolution, *supra* note 103, art. 3.
[112] *Id.*, art. 4.
[113] *Id.*, art. 3(g).
[114] *Id.*, art. 3(c).
[115] Weisbord, *Conceptualizing Aggression*, *supra* note 43, at 37.
[116] *Id.*
[117] *Id.*
[118] SWGCA 2009 Report, *supra* note 107.
[119] *See infra* text accompanying notes 133–37.

their definition to cyber warfare. Yet cyber warfare certainly has the potential to create catastrophic damage well beyond that resulting from a threshold traditional weapons attack. The interpretation of the list as open could conceivably include cyber attacks resulting in physical damages, but may not include the significant threat of non-lethal communication and economic disruption through cyber tactics.

¶36 The SWGCA definition also includes a de minimus clause, by limiting the definition to acts which, "by [their] character, gravity and scale, constitute[] manifest violation[s] of the Charter of the United Nations."[120] The de minimus clause provides an important qualifier for the regulation of cyber attacks under the definition. Many cyber attacks do not rise to the level of activity to warrant involvement by the ICC.[121] The de minimus clause makes clear only manifest violations of the UN Charter would trigger culpability under the statute.

¶37 As discussed below, the leadership clause of the SWGCA definition contains language that could be strictly interpreted to limit its applicability to cyber warfare. The conduct verbs provide for a broad level of culpable activity including planning, preparation, initiation and execution, all of which are broad enough to include cyber attacks. However, these conduct verbs have unique implications in the cyber context. The cyber tactic of creating a 'trapdoor' in a networked system for easy future access may be a preparatory step for aggression. Yet that very same trapdoor may only be used for cyber-espionage, a legal activity.[122] This duplicitous use creates difficulty in attributing culpability through the use of the conduct verbs alone, and creates the necessity for a liability doctrine in the crime of aggression.

¶38 The SWGCA has multiple liability doctrines to choose from, including the common law tradition of conspiracy, the doctrines of superior responsibility, organizational guilt, or joint criminal enterprise (JCE).[123] The likely doctrine of choice appears to be JCE.[124] JCE has gained significantly in importance since its adoption by the International Criminal Tribunal for the former Yugoslavia, and was recently incorporated into the Rome Statute.[125]

---

[120] *Id.*
[121] Schmitt, *supra* note 33 at 897.
[122] For a discussion of espionage, customary international law, and cyberspace, see Anthony D'Amato, *International Law, Cybernetics, and Cyberspace, in* INTERNATIONAL LAW STUDIES, COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 33, at 59, 67–68.
[123] See Weisbord, *Conceptualizing Aggression*, *supra* note 43, at 54.
[124] *Id.* at 58–59.
[125] *Id.*

¶39 JCE eliminates the reliance on a formal chain of command found in the doctrine of superior responsibility, instead requiring participation in the criminal enterprise.[126] This aspect of JCE creates significant benefits in the cyber context. Few, if any, cyber attacks occur in organizations with a formalized chain of command. Instead, multiple members of an organization like the RBN create a cyber attack capability which is implemented on the decision of potentially different members. The system lacks a true hierarchy of decision making. JCE allows broad connections of culpability in these fluid organizations.

¶40 However, this breadth also creates significant problems. Unlike the concept of conspiracy, JCE does not require explicit agreement on a common plan.[127] Instead, the Court relies on the participants' "common purpose" to connect them to the Collective/State act.[128] This common purpose test creates difficulty in application to certain cyber tactics, as the breadth of the common purpose is determined in hindsight by the Court. The ease with which a cyber attacker can morph between various levels and forms of attack will undoubtedly create issues related to intent when determining the breadth of a JCE.

Substantial Involvement of Non-State Actors

¶41 The 1974 GA Resolution is limited in scope to acts committed by State actors.[129] Subsequent articles repeatedly include the limiting phrases "by a State" and "of a State."[130] While the definition includes indirect uses of force, asymmetric conflict[131] is only included if conducted by or on behalf of a State.[132] Article 7 makes clear the Resolutions' inapplicability to certain independence movements without recognized Statehood.[133]

¶42 The SWGCA drafters included Article 1 of the Resolution nearly verbatim in their definition of the specific act of aggression.[134] As discussed

---

[126] *Id.*
[127] *Id.*
[128] *Id.*
[129] 1974 Resolution, *supra* note 103, art. 1.
[130] *Id.*, pmbl., arts. 1–3.
[131] Asymmetric conflict is classically defined as an imbalance of traditional military power between the warring parties. Modern definitions include an asymmetry in international status. Asymmetric warfare includes terrorism, guerilla tactics, hostage taking, and other non-traditional tactics. *See generally,* Ekaterina Stepanova, *Terrorism in Asymmetrical Conflict*, 23 STOCKHOLM INT'L PEACE RES. INST. RES. REP. 1 (2008), *available at* http://books.sipri.org/files/RR/SIPRIRR23.pdf.
[132] 1974 Resolution, *supra* note 103, art. 3(g).
[133] *Id.*, art. 7.
[134] SWGCA 2009 Report, *supra* note 107.

above, the SWGCA included all Article 3 examples in the proposed definition. Although the drafters retained the language from Article 1 of the GA Resolution that refers to 'manifest violations' of the UN Charter, the SWGCA proposed definition replaces the GA Resolution's clear qualifier that the list is not exhaustive with the ambiguous phrase "any of the following acts."[135]

¶43 This change emerged as a balance between competing negotiating positions in the SWGCA over the issue of whether the list should be open or closed.[136] The language was chosen to establish the necessary principle of legality, while not precluding a reading of the list as open.[137] The final phrasing was the result of political negotiations, with the final interpretation to be left to the judges. The definition can and should be read as indicating the list is merely illustrative of actions currently accepted as aggression under customary international law.[138]

¶44 The links between the State/Collective act and the individual contain similar limitations as the definition of the State act. While the conduct verbs provide for a rather broad level of culpable activity including planning, preparation, initiation and execution,[139] its applicability is severely limited by the leadership clause.

¶45 The leadership clause is intended by the SWGCA to limit the applicability of the international crime of aggression to leaders and to exclude followers.[140] The definition specifically limits its application to "persons in a position effectively to exercise control or to direct the political or military action of a State."[141] The leadership clause also limits culpable conduct to those with direct control over political or military action of the State.[142]

¶46 The leadership clause provides significant limitations on the regulation of cyber attacks. The vast majority of cyber attacks are conducted by individuals with only tenuous affiliations to a collective.[143] Most of these attacks are conducted by individuals for either pecuniary gain or

---

[135] *Compare* 1974 Resolution, *supra* note 103, art. 4, *with* SWGCA 2009 Report, *supra* note 107.
[136] Weisbord, *Prosecuting Aggression*, *supra* note 105, 182–83.
[137] SWGCA 2009 Report, *supra* note 107.
[138] Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27); Weisbord, *Prosecuting Aggression*, *supra* note 105, 182–83.
[139] SWGCA 2009 Report, *supra* note 107.
[140] Weisbord, *Conceptualizing Aggression*, *supra* note 43.
[141] SWGCA 2009 Report, *supra* note 107.
[142] *Id.*
[143] Barnett, *supra* note 33, at 26.

notoriety.[144] The remaining attacks are conducted by loosely affiliated groups of people who lack any meaningful association.[145] Only the occasional attack is even suspected to be sponsored by or conducted by a State.[146] However, the number of suspected State sponsored cyber attacks continue to grow.[147] As States begin to weaponize cyberspace while independent entities continue to offer cyber attack services to the highest bidder, serious international aggression will occur in cyberspace. Nevertheless, significant cyber attacks are more likely to be carried out by groups unaffiliated with particular States.[148]

¶47 Most hackers lack any ability to exercise direct control over another individual, and certainly not a collective entity. No hacker is the leader of a State. However, a hacker may be able to gain "effective control" of significant State assets. If the word "position" in the leadership clause is interpreted broadly, an individual hacker who launched a barrage of missiles or issued bogus orders for an invasion could fit within the leadership clause. The clause becomes more cumbersome when applied to more plausible scenarios. The opening of dams and rerouting of trains by a hacker would meet the "effective control" standard, but could easily be construed as outside the "political or military action" constraint. DDoS attacks, conducted by either individuals or collective actors, are also difficult to fit into the leadership clause.

¶48 However, some DDoS attacks may be viewed as meeting the restrictions of the leadership clause. A DDoS attack can control the military or political actions of a victim State by preventing the legitimate military and political leaders from exercising their control. The act of disrupting control itself is a form of control, through the maintenance of a status quo and the inability of the target State to react. Such a situation occurred in the Russia-Georgia conflict: the DDoS attacks prevented the Georgian government from effectively communicating with their own people and the outside world.[149] The party or parties responsible for the DDoS attacks "effectively control[led]" significant political actions of the State by crippling the State's ability to act. Had the DDoS attack also prevented the Georgian armed forces from coordinating an armed response, the State would have effectively lost control of its own military.

¶49 While some cyber attacks could be viewed as meeting the leadership clause, most are hampered by the requirement of State action.

---

[144] *See generally* Solce, *supra* note 20.
[145] *See generally id.*
[146] *See generally id.*
[147] *See generally id.*
[148] *See generally id.*
[149] Markoff, *supra* note 4.

Elimination of ICC jurisdiction over individuals and non-State actors for the crime of aggression leaves significant and more likely cyber attacks outside the scope of international regulation. At a minimum, State leaders authorizing cyber attacks should be held accountable when their actions create significant international repercussions.

The Disaggregation of Warfare

¶50 The SWGCA definition of the act of aggression, through borrowing heavily from the 1974 GA Resolution, continues the traditional emphasis on classic, aggregated warfare. The definition uses the movement of armies, the blockade by navies, and the sending of armed groups as examples of aggressive acts.[150] Allowing an attack by a State to originate from its sovereign territory is also considered an act of aggression.[151]

¶51 Cyber warfare, on the other hand, represents a disaggregation of combatants. The inherent nature of many cyber tactics requires significant geographic dispersal of assets. The identity and location of attackers are masked, creating substantial difficulty in determining the identity or location of the attackers. The potential liability by a State for allowing its territory to be used for the origination of an aggressive act creates interesting questions in the context of cyber warfare. Botnets are created and used across geographic borders, resulting in multiple States hosting the aggressive forces. Inadvertent hosting of assets used in cyber aggression would certainly not lead to liability. However, a duty might be construed against a State to assist in ending the aggression. Because Paragraph 2 (f) specifically includes allowing territory to be used in an aggressive attack, States who knowingly allow aggressive action to originate within their jurisdiction could be considered aggressors under the SWGCA proposed definition.[152] Paragraph 2(g) expands this to include allowing territory to be used by armed bands that launch attacks on another country.[153] Without significant interpretative expansion, the definition can be read to include a State who knowingly allows aggressive attacks to continually originate from botnets within its territory.

¶52 The international community must also determine the appropriate method for dealing with the modern weapons suppliers and mercenaries of the Internet. The development of malicious software and the sale of vulnerability information has become a global enterprise. Individuals who develop malicious software or sell software bugs to the highest bidder must also be held accountable. Without their assistance, large scale aggressive

---

[150] SWGCA 2009 Report, *supra* note 107.
[151] *Id.*
[152] *Id.*
[153] *Id.*

cyber attacks would be impossible. The SWGCA definition would treat these industrialists of the cyber age similarly to how prosecutors at Nuremburg treated the leaders of German industry.

¶53 The prosecutors at Nuremburg pursued charges against the financial and industrial leaders in Nazi Germany. Labeled the "economic case," the prosecutors viewed these leaders as sharing culpability for the war.[154] Industrialists and financers gave Hitler the necessary means to rearm Germany with full knowledge of his goal to expand German borders.[155] Although the "economic case" resulted in acquittals for all but one defendant,[156] the precedent is an important one. By allowing trials to proceed, the Nuremburg tribunal explicitly recognized the prima facie case of individual accountability for aggression outside of the traditional State structure.

¶54 As the emerging cyber battlefield gains importance, the individuals with roles most similar to the Nuremburg economic defendants will not be the manufacturers of the computers, but the bug hunters and the leaders of the RBN. However, under the SWGCA's definition, these individuals are only included when their acts interface with State-sponsored cyber aggression. Their actions would be viewed as impertinent to the international system should they sell cyber assets or develop malicious programming solely for non-State actors.

¶55 The likely choice by the SWGCA to include JCE as the standard for liability in the crime of aggression eliminates many of the issues associated with the disaggregation of warfare. By removing the common-law conspiracy requirement for agreement to achieve a collective purpose, the significant contributors to cyber weaponry can be held liable for their acts. The leaders of organizations who commit criminal acts that have a foreseeable consequence of aiding cyber aggression would be considered part of the JCE.

New Conceptions of Territoriality

¶56 The SWGCA definition makes frequent reference to territory.[157] Paragraph 1 limits the definition of aggression to acts directed at the sovereignty, territorial integrity or political independence of another State.[158] The examples described in paragraph 2 rely heavily on territory,

---

[154] TELFORD TAYLOR, THE ANATOMY OF THE NUREMBERG TRIALS 81 (Knopf 1992).
[155] *Id.*
[156] Weisbord, *Prosecuting Aggression*, *supra* note 105, at 165 nn. 21–25. The one leader convicted, Roechling, won his case on appeal. *Id.*
[157] *See generally* SWGCA 2009 Report, *supra* note 107.
[158] *Id.*

using the term seven times.[159] For example, the paragraph refers to the invasion or attack of territory, the annexation of territory, and the bombardment of territory. Blockades are limited to ports and coasts.[160]

¶57 The frequent references to territory continue the traditionalistic trend of the SWGCA definition. Cyber attacks will rarely conform to historic conceptions of territory. Attacks can be triggered from any location with Internet access. Botnets can easily be transcontinental. The consequences of suspected Chinese disruption of North American power grids affected both Americans and Canadians.[161] The origins, staging, targets, and consequences for these attacks will not be contained neatly within the borders drawn on a map.

¶58 The leadership clause, conduct verbs, and use of JCE contain no explicit limitations to traditional notions of territoriality. Judges should refrain from transposing the territorial references of the second paragraph's definition of aggressive acts to the first paragraph's definition of the crime of aggression. The abilities of leaders to orchestrate aggressive acts outside the limitations of traditional territoriality extend beyond cyber warfare. An exiled leader who orchestrates an aggressive act with conventional weaponry should face the same consequences as a sitting leader who gives orders from his capital city.

¶59 Both territorial issues and the structure of the Internet create significant challenges for the application of the Rome Statute's jurisdictional trigger to cyber attacks. Generally speaking, the ICC will invoke jurisdiction when a signatory party is either the aggressor or victim of an act that meets the definition.[162] Article 12 of the Rome Statute creates jurisdiction when the conduct occurs in or is committed by a national of a signatory State.[163] It also includes the vessels and aircraft of the signatory States.[164] The SWGCA has generally agreed that Article 12 includes both

---

[159] *Id.*
[160] *Id.*
[161] Gewirtz, *supra* note 59.
[162] SWGCA 2009 Report, *supra* note 107. This statement is severely complicated by the ability for States to be parties to the Rome Statute but not accept the crime of aggression. For more on the current status of these discussions, please see SWGCA 2009 Report, *supra* note 107, Appendix II *Non-paper on other substantive issues on aggression to be addressed by the Review Conference*, Part III. For the purposes of this article, this complicating factor has been eliminated. These complications add nothing of substance to the analysis of cyber attacks and aggression.
[163] Rome Statute of the International Criminal Court, art. 12, July 17, 1998, 2187 U.N.T.S. 90.
[164] *Id.*

the territory of the conduct and the consequence, ensuring liability for missile attacks and other remote strike capabilities.[165]

¶60 While these clarifying remarks provide sufficient jurisdictional guidance for traditional weaponry, the question is greatly complicated by the internet's structure. The natural flow of information on the internet creates unpredictable routing through various jurisdictions. A cyber attack will nearly certainly be routed through a large number of territories. The Court must determine whether such routing creates sufficient "conduct" to create jurisdiction of the court. Further, the relocation of Georgian websites to the United States creates another example of jurisdictional difficulty. The cyber attacks that occurred after the move attacked not Georgia's, but an American company's equipment. The crime of aggression in cyberspace creates the question of whether the territory should be virtual, actual, or both.

III. PRESCRIPTIONS, PROPOSALS AND SUGGESTIONS FOR THE ASSEMBLY OF STATES PARTIES AT THE 2010 REVIEW CONFERENCE

A new form of warfare

¶61 To sufficiently counter the emerging challenges of cyber attacks, the ASP must adopt a framework that can be interpreted as inclusive of non-traditional attacks by non-traditional actors. This framework will likely require a normative shift, focusing on the consequences of collective acts rather than the instrumentalities used in their execution.

¶62 Professor Michael Schmitt, in a 1999 article, examined the use of force framework established by the UN Charter in light of the then-recent emergence of computer network attacks.[166] According to Schmitt, the UN Charter drafters truly wished to regulate consequences of State action.[167] Yet the necessity to articulate workable normative standards required them to instead pursue restrictions on instrumentalities.[168] Instrumentalities include the use of military, economic, and diplomatic force.[169] By regulating instrumentalities, the drafters sought indirectly to regulate the consequences of their use.[170] However, cyber attacks no longer fit neatly into these preexisting divisions. Rather, the diversity of potential cyber attacks spans the range of consequences. As cyber attacks no longer fit neatly into the preexisting divisions of instrumentalities, Schmitt argues that

---

[165] SWGCA 2009 Report, *supra* note 107.
[166] *See generally* Schmitt, *supra* note 33.
[167] *Id.* at 900.
[168] *Id.* at 908.
[169] *Id.* at 909.
[170] *Id.* at 910.

the best approach is to shift the normative framework by deconstructing those instrumentalities back to their original "community values."[171] These values can then be used as shorthand to determine the legality of various levels of cyber attack.[172]

¶63 A normative framework shift is vital to international law's adaptation to cyber warfare. Without it, the current prohibitions on force lack sufficient breadth to adequately address the many forms of cyber attack. However, Schmitt's proposal suffers from a significant flaw—the process of applying consequences inherently requires waiting for the actions to occur. While the proposal may be sufficient to cast judgment on past action, the process raises serious and important questions regarding the Rome Statutes principle of legality. Even to the attacker the consequences of a cyber attack may be unknown at the time the attack is triggered. More importantly, cyber tactics have shown a disturbing flexibility in swiftly shifting between legal and illegal international acts. A State faced with potential cyber aggression cannot wait for the consequences of the aggressive act when determining the appropriate reaction.

¶64 Analogizing cyber tactics to those of traditionally recognized aggressive acts would be an alternative to Schmitt's proposal. For example, a DDoS attack that disabled electronic commerce could be analogized to a blockade of a port. However, the analogy approach would violate the principle of *nullum crimen sine lege* codified in Article 22 of the Rome Statute.[173] Article 22 requires the definition of a crime be strictly construed and not extended by analogy.[174] Further, while the analogy approach would include cyber attacks that cause physical damage similar to traditional attacks, analogy would fail to include the more likely attacks that merely cause costly and significant disruption of economic and communications systems.

¶65 Broad interpretation of the term "armed" is a second alternative.[175] By including non-traditional armaments in the term, the definition broadens significantly without any further revision.[176] The de minimus clause serves as a protection against over inclusion.[177] Article 22 of the Rome Statute would not prevent this expansion, as the broad interpretation of "armed" is not accomplished through analogy.[178] Both of these alternatives fail to

---

[171] Schmitt, *supra* note 33, at 910.
[172] *Id.* at 912.
[173] Rome Statute of the International Criminal Court, art. 22, July 17, 1998, 2187 U.N.T.S. 90.
[174] *Id.*
[175] *See* Weisbord, *Conceptualizing Aggression*, *supra* note 43, at 40.
[176] *Id.*
[177] *Id.*
[178] *Id.* at 40–41.

address the greatest flaw in Schmitt's proposal—the flexibility of cyber tactics. States faced with a decision of how to respond to a cyber attack that could quickly morph into a clearly aggressive act lack guidance on the appropriate response. Further guidance on this issue will likely need to come from another international body.

¶66 Key to any such solution is the interpretation of the SWGCA definition as containing an 'open' exemplary list of aggressive acts. A normative shift provides a base for constraining the use of cyber attacks in modern warfare, but the shift alone is insufficient to deal with the increased individuality of cyberspace. Presumably, Schmitt would continue to use the traditional concept of State actor in determining the applicability of international restrictions.

Substantial Involvement of Non-State Actors

¶67 The ongoing SWGCA attempt to define the crime of aggression provides an excellent opportunity to not only shift the normative framework for the conceptualizing use of force, but also provide for individual accountability on a global scale. The ASP should embrace the concept of individual responsibility for the actions of non-State actors and reject the artificial limitation to State actions. Combining this alteration with an articulation of a consequence-based normative framework will greatly enable the international community to adapt the crime of aggression to some of the greatest challenges threatening world peace and stability.

¶68 Davis Brown considered—and ultimately rejected—the use of the ICC to combat the growing threat of cyber warfare.[179] In dismissing the ICC, Brown cited the inflexibility of Article 22 of the Rome Statute.[180] Since Article 8 of the Rome Statute contains an extensive list of specific acts considered 'war crimes,' those occurring in cyberspace would not be included in the court's jurisdiction. Instead of the ICC, Brown argued any new convention should refer disputes to the ICJ[181] More states are likely to sign such a convention as it bypasses resistance to the ICC from key players, such as China and the United States.[182]

¶69 Brown's criticism of the ICC fails to consider two important issues.[183] The first is the ability of the ICC to mold the crime of aggression

---

[179] Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 212 (2006).
[180] *Id.*
[181] *Id*. at 213.
[182] *Id.*
[183] *See id.*

to include this very real and very likely future battlefield.[184] Brown's criticism of the inflexibility of the Rome Statute and its principle of *nullum crimen sine lege* may prove accurate for war crimes. However, by drafting a definition that includes aggressive acts in cyberspace, the ASP can bypass Brown's critique of the current Statute. The definition of the crime of aggression represents an important opportunity to provide the statute much needed relevance throughout the twenty-first century.

¶70 Secondly, Brown's suggestion of referring disputes to the ICJ eliminates the ability of the international community to hold individuals accountable for their aggressive acts. Brown admits that the ICJ lacks the power to directly regulate individual behavior, but prefers the ICJ as a means of bringing as many countries into his proposed convention as possible.[185] While such an effort at compromise is admirable, it ignores the greatest issue with regulating cyber warfare: the ease with which non-State collectives can engage in devastating asymmetric warfare with low costs and high levels of anonymity.[186]

¶71 Brown's overall recommendation of developing a Law of Armed Conflict for cyberspace remains a popular one.[187] While the applicability of certain aspects of *jus in bello* provide unique challenges and likely will require significant amendment or addition, such efforts fail to deal with the larger problem of *jus ad bellum* that provide a greater risk to the international community. The ASP's task of drafting a definition of aggression provides the necessary opportunity to both update the *jus ad bellum* for the new battlefield while simultaneously creating individual responsibility for those acts.

¶72 The ASP should consider expanding the crime of aggression to include actions by non-State actors, as they have done with other international crimes. The realities of cyberspace greatly increase the ability of non-State groups to regularly and devastatingly function as aggressive actors in the international system. The ASP should provide the ICC with the capability of prosecuting all individuals responsible for the aggressive acts of collectives.

The Disaggregation of Warfare

¶73 The disaggregation of warfare in cyberspace alone provides limited challenges for the SWGCA definition. The SWGCA decision to include expansive conduct verbs and both effective and direct forms of leadership,

---

[184] *See* Brown, *supra* note 179, at 213.
[185] *See id.* at 214.
[186] *See* Gewirtz, *supra* note 59.
[187] *See generally* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023 (2007).

combined with the presumed use of a JCE standard allow the definition to apply equally to all leaders of an aggressive cyber act. The difficulties from the disaggregation of warfare derive from the interplay of disaggregation with the other characteristics of cyber attacks. Disaggregation is the factor that underscores the importance of moving past a State-centric definition that includes simplistic concepts of territoriality, and reliance on outdated examples of aggressive action. Disaggregation is the factor that requires a reexamination of these other aspects of the definition. Disaggregation requires the leadership clause and conduct verbs be interpreted broadly, in a manner consistent to effectuate other adjustments in the definition of the crime of aggression.

New Conceptions of Territoriality

¶74 Cyberspace and its new territoriality create largely conceptual rather than practical requirements for the definition of aggression. The definition should shift significantly from that of the 1974 GA Resolution and reject the archaic rigidity of territoriality. The prosecutors and judges of the ICC will be faced with difficult jurisdictional questions stemming from the evolving conceptions of territory and cyberspace. The breadth of ICC jurisdiction can be greatly increased if the physical routing of attacks is considered when determining whether a State party to the Rome Statute was attacked. Including both the State victim in cyberspace and the State whose physical assets are attacked creates broader jurisdictional opportunities. Regardless of the interpretative decisions, they must be logically compatible. An interpretation that disregards the physical routing of cyber attacks must also disregard the physical location of the servers hosting the victim State's cyber assets.

V. CONCLUSION

¶75 The threats posed by cyber attacks continue to expand with new technological developments. Cyber attacks display a new form of conflict, allow for aggression by non-State collective actors, demonstrate significant disaggregation of warfare, and challenge the traditional concepts of territory. In light of these sociological changes to warfare, the ASP should adjust the emerging definition of aggression to ensure its relevance to future conflicts. Global reliance on computer networks and the internet will only increase. As more States integrate their infrastructure, the ferocity of cyber warfare will escalate. The ICC should be equipped to dampen, if not punish, these attacks.

¶76 This iBrief has the narrow purpose of demonstrating the necessity of making a definition of the crime of aggression sociologically relevant for the likely conflicts of the future. The ICC will be only a part of a solution to this new threat to international security. An intersecting web of

organizations and collaborative efforts will be necessary to fully address the issue. However, this iBrief's analysis of the SWGCA's proposed definition demonstrates an important lesson. The designers of international legal frameworks must consider emerging sociological forces when drafting their language. The sociological forces will significantly shape the environment in which the new institutions operate. Further, the implementers of those frameworks—the officers of the new institutions—must be given the flexibility to adapt them to the challenges of tomorrow.