ARTICLES

THE KAMPALA COMPROMISE AND CYBERATTACKS: CAN THERE BE AN INTERNATIONAL CRIME OF CYBER-AGGRESSION?

KEVIN L. MILLER*

I. INTRODUCTION

At the Kampala Review Conference in 2010, after decades of delay and debate, the States Parties to the Rome Statute finally agreed on a definition of the crime of aggression acceptable for prosecuting individuals at the International Criminal Court ("ICC"). Reactions to the new definition have been mixed,[1] and many scholars have expressed concern that the new crime will have narrow applicability to modern conceptions of warfare.[2] Cyberattacks, drone strikes, and chemical and biological attacks, conducted by both state and non-state actors, fit poorly into traditional conceptions of warfare drawn from World War II and the Cold War.

* Kevin Miller is a third-year law student at the University of Florida Levin College of Law, where he is a member of the *Journal of Law and Public Policy* and the Bennett Inn of Court. Prior to attending law school, he was a software engineer and technology specialist for several technology companies, including Microsoft, and founded his own software company. He is also the author of a book on software development and has presented papers at several conferences.

1. Reactions run the gamut from hopeful to pessimistic. *See, e.g.*, Michael J. Glennon, *The Blank-Prose Crime of Aggression*, 35 YALE J. INT'L L. 71, 111–12 (2010) ("Given the failure of states to reach agreement on a specific, substantive core of conduct that a definition might delineate, the SWGCA [Special Working Group on the Crime of Aggression] chose to paper over differences in the hope that a consensus might emerge in the future. But in the imposition of criminal punishment, the papering over of differences is precisely what the principle of legality prohibits. Potential defendants have a right to know the specific elements of a crime before their conduct occurs—not when they are charged or tried, after a consensus has finally emerged."). *But see* Noah Weisbord, *Judging Aggression*, 50 COLUM. J. TRANSNAT'L L. 82, 108 (2011).

2. *See, e.g.*, M. CHERIF BASSIOUNI, INTRODUCTION TO INTERNATIONAL CRIMINAL LAW 671 (2d rev. ed. 2013).

This Article considers whether the definitions adopted at Kampala[3] can be applied to cyberattacks and therefore used to decelerate the arms race in an increasingly aggressive cyberspace. After briefly reviewing the history behind the crime of aggression, this Article examines several recent cyberattacks with the goal of clarifying the key differences between cyberattacks and conventional attacks. It argues that the definitions at Kampala can be flexibly interpreted by the ICC judges to encompass cyber-aggression. However, the meanings of key terms in the definition of aggression inevitably will undergo further development through international standards-setting efforts and state practice. This Article argues that U.S. practice in particular is expanding the definition, paradoxically making U.S. actions more likely to be perceived as cyber-aggression, and that U.S. policy should be reshaped in light of its influence on this developing area of international law. This Article then considers whether the crime of aggression's threshold clause forms a barrier to the prosecution of cyberattacks. Ultimately, the author concludes that, at least for the time being, practical and jurisdictional barriers will likely forestall any application of the crime of aggression in the context of cyber-aggression. Consequently, several other methods should be simultaneously pursued by international groups to promote a peaceful cyberspace.

II. A BRIEF HISTORY OF THE CRIME OF AGGRESSION

The judges at the Nuremberg Tribunal called aggression "the supreme international crime," perceiving that aggression by one nation against another—whether motivated by politics, power, or demand for resources—formed the wellspring for the hatred from which many other heinous crimes flowed.[4] However, for decades international bodies struggled in articulating why, precisely, "aggression" warranted punishment of either individuals or states. In 1998, 120 nations signed the Rome Charter,[5] establishing a permanent ICC and formally defining genocide, crimes

3. Often referred to as the "Kampala compromise." Stefan Barriga, *Negotiating the Amendments on the Crime of Aggression*, *in* THE TRAVAUX PRÉPARATOIRES OF THE CRIME OF AGGRESSION 3, 3 (Stefan Barriga & Claus Kress eds., 2012).

4. JUDGMENT OF THE INTERNATIONAL MILITARY TRIBUNAL FOR THE TRIAL OF GERMAN MAJOR WAR CRIMINALS 13 (1946).

5. *Rome Conference*, COALITION FOR THE INT'L CRIM. CT. WEBSITE, http://www.iccnow.org/?mod=rome (last visited Oct. 3, 2013). The U.S. and China voted against the adoption of the Rome Charter. *Id.* The U.S., China, and Russia are not States Parties to the Rome Charter. *Id.*

against humanity, and war crimes, so that they could be prosecuted. Despite prior setbacks, the parties to the Rome Charter still instinctually felt that "aggression" was blameworthy—so much so that they voted into the Rome Charter a placeholder, Article 5(2), which allowed the parties to proceed with respect to the already defined crimes and postpone the formal definition of a crime of aggression.[6] The parties then resolved to work on the definition to present a proposal at the 2010 Review Conference.[7]

For twelve years the parties struggled to define "aggression," starting in the third session of the Preparatory Commission[8] and proceeding through over a dozen meetings of the Special Working Group on the Crime of Aggression ("SWGCA").[9] The meetings were initially marked by negativity and mistrust, but gradually common ground formed as the parties began to work with concrete proposals instead of political abstractions.[10] There were several questions that made the negotiations contentious.

First, what would be the quantitative and qualitative limits to the crime? Some states wished to limit criminal responsibility only to "wars of aggression," while others preferred a more expansive view. Second, what was the nexus between the state's act and the individual's act? Third, what would be the relationship of the ICC to the United Nations ("U.N.") Security Council (the "Council"), which had the power under the U.N. Charter to label a state as aggressive and take action? Fourth, when would jurisdiction for the crime of aggression under the ICC become activated? Fifth, which parties could be prosecuted for aggression under the Rome Charter?[11]

6. Rome Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 90, *available at* http://untreaty.un.org/cod/icc/statute/romefra.htm [hereinafter Rome Statute] (entered into force July 1, 2002). Article 5(2) states: "The Court shall exercise jurisdiction over the crime of aggression once a provision is adopted in accordance with articles 121 and 123 defining the crime and setting out the conditions under which the Court shall exercise jurisdiction with respect to this crime. Such a provision shall be consistent with the relevant provisions of the Charter of the United Nations." *Id.*

7. Resolution F of the Final Act of the United Nations Diplomatic Conference of Plenipotentiaries on the Establishment of an International Criminal Court, July 17, 1998, U.N. Doc. A/CONF.183/10, *available at* http://untreaty.un.org/cod/icc/statute/finalfra.htm.

8. The Preparatory Commission (1999-2002) had the mandate of making the practical arrangements for beginning the Court's operations. Barriga, *supra* note 3, at 8.

9. The SWGCA was formed to work specifically on defining the crime of aggression.

10. *See* Barriga, *supra* note 3, at 9.

11. *See generally id.* at 14–57.

Over time, the parties narrowed down answers to these questions. After lengthy negotiations during the two-week period of the Review Conference in Kampala, Uganda, the parties adopted Resolution RC/Res.6 defining the crime of aggression in the late evening of June 11, 2010.[12] RC/Res.6 introduces a new Article 8 *bis* into the Rome Charter, defining the crime of aggression by deferring substantially to a prior document, General Assembly Resolution ("G.A. Resolution") 3314.[13] This is supplemented by Annex II, containing the elements of the crime of aggression.[14] Articles 15 *bis* and 15 *ter* define how potential crimes of aggression get referred to the ICC, specifying a two-pronged approach which differs substantially depending on whether the U.N. Security Council refers the case or whether the ICC Prosecutor or a victim State refers the case. Annex III of the resolution contains "Understandings," which further clarify the meanings that the parties intended in some paragraphs of the articles.[15] Notably, jurisdiction is also subject to two additional criteria: first, the ICC only has jurisdiction over crimes of aggression committed one year after thirty States Parties have ratified the amendments;[16] and second, the States Parties must vote again, by two-thirds majority, to "enact" jurisdiction, and this vote cannot be held before January 1, 2017.[17]

The Kampala Compromise, as it is often called, crafted intermediate positions on many contentious points, leaving much interpretive work to be done by jurists, scholars, the ICC, and back-channel conversations between the ICC and the U.N. Security Council. In the words of one commentator:

> In order to achieve an agreement among rival nations, the [Assembly of States Parties] employed a number of drafting techniques, including the use of "constructive ambiguity," in the language of the compromise where nations could not reach specific agreement. The practical result, for better

12. Res. RC/Res.6, U.N. Doc. RC/Res.6 (June 11, 2010), *available at* http://www.icc-cpi.int/iccdocs/asp_ docs/Resolutions/RC-Res.6-ENG.pdf [hereinafter Kampala Compromise] (adopting the crime-of-aggression amendments to the Rome Statute).

13. *Id.*

14. *Id.*

15. *Id.*

16. *Id.* at art. 15 *bis*, para. 2. As of October 2013, five States Parties—Liechtenstein, Samoa, Trinidad and Tobago, Luxembourg, and Estonia—have ratified the amendments in their own countries. *Status of Ratification and Implementation of the Kampala Amendments on the Crime of Aggression Update No. 7* (Apr. 10, 2013), http://crimeofaggression.info/documents//1/Status_Report-ENG.pdf.

17. *Id.*

> or for worse, was to transfer the task of interpreting the definition of the crime of aggression and its jurisdictional conditions to the ICC judges.[18]

To address balance-of-power concerns between the ICC and the U.N. Security Council, for example, the drafters created a two-part scheme which allows a victim State or the ICC Prosecutor to refer a case against an aggressor State to the Rome Charter only when the latter has *not* "opted out" of jurisdiction by lodging a declaration.[19] Either or both parties may have ratified the amendments, so long as the aggressor did not opt out.[20] Further, the Prosecutor must submit the act in question to the U.N. Security Council for determination on whether it qualifies as "aggressive" and give the Council six months to rule on the matter.[21] If, after six months, the Council has not ruled, the Prosecutor may proceed.[22] If the U.N. Security Council rules that the act is not aggression, then the Prosecutor may likely also proceed, unless the U.N. Security Council invokes its Article 16 power of "deferral" of prosecution for renewable one-year periods.[23] In contrast, under the second method of referral, the U.N. Security Council has broad authority to recommend an act of aggression for prosecution to the ICC whether or not the perpetrator or victim States are even parties to the Rome Charter.[24]

The intricacies of these conditions form a significant barrier to the enactment of jurisdiction against any aggressive act, but are only tangentially relevant here. More salient to our discussion of the crime of aggression in the context of cyber-operations are the compromises and ambiguities in the "act of aggression" itself and in the interpretation of the link between state and individual action in these new and unusual forms of attack. After a brief foray through the world of recent cyberattacks, this Article will turn to those questions.

18. Weisbord, *Judging Aggression*, *supra* note 1, at 86.

19. Kampala Compromise, *supra* note 12, art. 15 *bis*, para. 4.

20. *Id.*

21. *Id.* at art. 15 *bis*, para. 6–8.

22. *Id.*

23. *Id.* at art. 16.

24. *Id.* at ann. III, para. 2. Considering that a unanimous vote of the U.N. Security Council is required, there is probably little hope that any of the non-parties who are permanent members of the Council (Russia, China, and the U.S.) will vote to refer their own act of aggression using this form of jurisdiction.

III. CHARACTERIZING CYBERATTACKS—HACKING, VIRUSES, AND ESPIONAGE

A. RECENT EXAMPLES

Stuxnet. On June 17, 2010, a Belarusian antivirus company reported the existence of a new computer worm it had found on the computers of its Iranian customers.[25] Over the course of several months, it became apparent to security experts that the worm was actually a sophisticated piece of malware whose ultimate goal was to surreptitiously affect the operation of the nuclear centrifuges at Iran's Natanz nuclear fuel enrichment facility.[26] It achieved this by infecting the process control software that tuned the speed of the spinning centrifuges; the malware would start and stop the centrifuges rapidly and also cause them to spin at speeds outside their proper operating ranges, all while reporting back to the operator that everything was normal.[27] The malware achieved its goals, destroying a thousand centrifuges completely and taking additional thousands out of operation; the total impact was to set back the Iranian nuclear program twelve to eighteen months.[28] Over the next two years, culminating in mid-2012, it became clear that the malware was created through a joint effort of the U.S. government and Israel's Mossad called "Operation Olympic Games."[29] The operation had begun under President George W. Bush and was continued by and released under the orders of President Barack Obama.[30]

2007 Estonia Cyberattacks. In late April 2007, a series of cyberattacks targeted government, financial, and news media websites in the Baltic state of Estonia.[31] The attacks occurred during a war of words with Russia over

25. Nicholas Falliere et al., *W32.Stuxnet Dossier Version 1.3*, WIRED (Nov. 2010), *available at* http://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf.

26. *See* Holger Stark, *Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War*, SPIEGEL ONLINE INT'L (Aug. 8, 2011), http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912-2.html.

27. *Id.*

28. *Id.*

29. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all.

30. *Id.*

31. Nate Anderson, *Massive DDoS Attacks Target Estonia; Russia Accused*, ARSTECHNICA (May 14, 2007), http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/.

Estonia's relocation of the Bronze Soldier of Tallinn, a Soviet-era monument.[32] The attackers defaced several websites, but most of the attacks utilized Distributed Denial of Service ("DDoS") methods.[33] At the time, the cyberattacks represented the largest and most sophisticated onslaught to date, as well as one of the first to attack most of a country's entire infrastructure."[34] Accusations flew against the Russians, but because the Estonian government lacked any concrete evidence of attribution, the Russians denied involvement.[35] Post-event analysis of culpability has been inconclusive, with experts in one camp concluding that the attacks were sophisticated enough to have required the involvement of the Russian state, and experts in the other camp claiming that the attacks were likely the work of Russian nationalist sympathizers.[36]

2008 Georgian Cyberattacks. In the three weeks leading up to the August 8, 2008 incursion by the Georgian military into the semi-autonomous South Ossetia region, a stream of cyberattacks struck Georgian government websites.[37] The Georgian Parliament's websites were hacked and replaced by images that compared the Georgian president to Adolf Hitler.[38] Other civilian and news websites were attacked using DDoS.[39] Russian government involvement was suspected, though Russian officials denied it.[40] Several security researchers, analyzing post-attack Internet traffic, have concluded that the attacks were probably coordinated by

32. *Id.*

33. A denial-of-service attack attempts to make a network resource unavailable to its intended users by flooding the target resource with unimportant or useless requests. A distributed denial-of-service attack makes the attack more powerful by using thousands or millions of machines to flood the target. *DDoS Attack*, WEBOPEDIA, http://www.webopedia.com/TERM/D/DoS_attack.html (last visited Oct 2, 2013).

34. Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

35. Anderson, *supra* note 31.

36. Bill Brenner, *Experts Doubt Russian Government Launched DDoS Attacks*, TECHTARGET (May 18, 2007), http://searchsecurity.techtarget.com/news/1255548/Experts-doubt-Russian-government-launched-DDoS-attacks.

37. John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html?em&_r=0.

38. Travis Wentworth, *You've Got Malice; Russian Nationalists Waged a Cyber War Against Georgia. Fighting Back Is Virtually Impossible*, NEWSWEEK INT'L EDITION (Sept. 1, 2008), http://www.thedailybeast.com/newsweek/2008/08/22/you-ve-got-malice.html.

39. *Id.*

40. *Id.*

Russian intelligence services.[41] The Russian military was likely leading the initial attack, while Russian nationalist sympathizers launched a second attack.[42] These attacks were significant because they were the first time in which a conventional war featured cyberattacks.[43]

2012 "Shamoon" Attacks. In mid-August of 2012, Saudi Arabia's national oil provider, Saudi Aramco, announced that it had been attacked by a computer virus.[44] This virus affected 30,000 of its employee's desktop computers and ceased company operations for a week.[45] The malware, dubbed "Shamoon," targeted a few companies in oil and gas production.[46] Shamoon seems to have been originally designed for espionage, but was then modified to destroy the files on infected computers and replace them with images of burning American flags.[47] Further analysis of the malware showed that it utilized a module called "Wiper," the same name used by a module of the "Flame" espionage malware.[48] Most experts believe that the same Israeli-U.S. team that created Stuxnet also created Flame to gather intelligence about the Iranian network infrastructure.[49] This discovery led many U.S. officials to conclude that Iran created Shamoon in retribution for Stuxnet and Flame.[50] To date, Shamoon is the most damaging cyberattack ever faced by a company.[51]

Chinese Army Hacks of U.S. Companies. Since 2006, a group of hackers has been conducting advanced, persistent espionage against at least one hundred companies in over twenty industries.[52] The hackers penetrated

41. John Leyden, *Russian Spy Agencies Linked to Georgian Cyber-Attacks*, THE REGISTER (Mar. 23, 2009), http://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis/.

42. *Id.*

43. *Id.*

44. Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back*, N.Y. TIMES (Oct. 23, 2012), http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

45. *Id.*

46. *Id.*

47. *Id.*

48. *Id.*

49. Kim Zetter, *Report: US and Israel Behind Flame Espionage Tool*, WIRED (June 19, 2012), http://www.wired.com/threatlevel/2012/06/us-and-israel-behind-flame.

50. Perlroth, *In Cyberattack on Saudi Firm*, *supra* note 44.

51. *Id.*

52. David E. Sanger et al., *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES (Feb. 18, 2013), http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?hp&_r=2&.

a company's network, hid out for months or years, and secretly stole passwords and proprietary corporate data.[53] Targets included Coca-Cola, Dell, and Telvent, a designer of software that allows oil, gas, and power grid companies remote control of valves and switches.[54] The Telvent hacking has particularly concerned security experts, since the breach, had it been successful, would have allowed access to the programming interfaces of industrial control systems used widely in the U.S. and Canada—much in the same way that Stuxnet targeted the software used to program nuclear centrifuges.[55]

In February 2013, a report by private cybersecurity firm Mandiant concluded that all of these attacks originated from a single group, the so-called "Comment Crew." The group was tracked to a small number of internet addresses based near Datong Road in Shanghai, in the proximity of a Chinese Army unit.[56] Although Mandiant was unable to link the use of the addresses directly to individuals inside the building, the firm established that circumstantial evidence of the Chinese Army's involvement is conclusive.[57] Chinese officials have responded by denying the allegations, insisting that they themselves are under constant attack from American internet addresses and suggesting that they were hacked to make it seem as though the attacks originated in China.[58] A later report claimed that China was behind 96% of all incidents of cyber-espionage.[59]

53. *Id.*

54. *Id.*; Kim Zetter, *Maker of Smart-Grid Control Software Hacked*, WIRED (Sept. 26, 2012), http://www.wired.com/threatlevel/2012/09/scada-vendor-telvent-hacked.

55. Zetter, *Report: US and Israel Behind Flame Espionage Tool*, *supra* note 49. President Obama, in his 2013 State of the Union Address, noted: "We know foreign countries and companies swipe our corporate secrets . . . . Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air-traffic control systems." *Id.*

56. MANDIANT CORP., APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 2–3 (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf [hereinafter MANDIANT REPORT].

57. Kevin Mandia, CEO of Mandiant, said: "Either they are coming from inside Unit 61398, or the people who run the most-controlled, most-monitored Internet networks in the world are clueless about thousands of people generating attacks from this one neighborhood." Sanger et al., *supra* note 52.

58. David Barboza, *China Says Army Is Not Behind Attacks in Report*, N.Y. TIMES (Feb. 20, 2013), http://www.nytimes.com/2013/02/21/business/global/china-says-army-not-behind-attacks-in-report.html?ref=technology.

59. Craig Timberg, *Vast Majority of Global Cyber-Espionage Emanates from China, Report Finds*, WASH. POST (Apr. 22, 2013), http://www.washingtonpost.com/business/technology/vast-majority-of-global-cyber-espionage-emanates-from-china-report-finds/2013/04/22/61f52486-ab5f-11e2-b6fd-ba6f5f26d70e_story.html ("Of 120 incidents of government cyber-espionage detailed in the report, 96 percent came from China; the source of the other 4 percent was unknown."). Interestingly,

South Korean Bank Attacks. Even more recently, on March 20, 2013, banks and broadcasting companies in South Korea were attacked by a logic bomb that wiped the hard drives of company computers and put a number of ATMs out of operation.[60] The malware contained code targeted both at desktops and server computers.[61] More than 50,000 computers were affected. In April, South Korea accused the North Korean intelligence agency of launching the attack as a response to a joint South Korean-U.S. military exercise.[62] Meanwhile, the hacker collective Anonymous retaliated by targeting a North Korean state news agency for alleged war-mongering.[63] North Korea responded to these claims by denying involvement and threatening "thermonuclear war" against the South.[64]

AP Twitter Hack Affects U.S. Stock Market. On April 23, 2013, hackers hijacked the Twitter account of the Associated Press and posted a fake tweet stating that explosions at the White House had injured President Obama.[65] Automated futures trading programs, set up to react quickly to world news, took over for several minutes and performed a sell-off, erasing $136 billion from U.S. stock market valuations.[66] A group calling itself the Syrian Electronic Army has claimed responsibility, but the real perpetrators are currently unknown.[67]

that report also said the high incidence was in part because Chinese groups tended to reuse techniques more often, making them easier to identify than other groups. *Id.*

60. Kim Zetter, *Logic Bomb Set Off South Korea Cyberattack*, WIRED (Mar. 21, 2013), http://www.wired.com/threatlevel/2013/03/logic-bomb-south-korea-attack/.

61. *Id.*

62. *South Korea Blames North for Bank and TV Cyber-Attacks*, BBC NEWS (Apr. 10, 2013), http://www.bbc.co.uk/news/technology-22092051; Sean Gallagher, *North Korean Military Blamed for "Wiper" Cyber Attacks Against South Korea*, ARSTECHNICA (Apr. 10, 2013), http://arstechnica.com/security/2013/04/north-korean-military-blamed-for-wiper-cyber-attacks/.

63. Jon Brodkin, *Anonymous Hackers Take Control of North Korean Propaganda Accounts*, ARSTECHNICA (Apr. 4, 2013), http://arstechnica.com/security/2013/04/anonymous-hackers-take-control-of-north-korean-propaganda-sites/.

64. *Id.*

65. Nicole Perlroth, *Investigations Expand in Hacking of A.P. Twitter Feed*, N.Y. TIMES (Apr. 24, 2013), http://bits.blogs.nytimes.com/2013/04/24/investigations-expand-in-hacking-of-a-p-twitter-feed/.

66. *Id.*

67. *Id.*

B. GENERAL CHARACTERISTICS OF CYBERATTACKS

The aforementioned events are merely a sampling of the types of cyberattacks that have occurred over the past several years. A comprehensive list would number well into the hundreds.[68] There are also dozens of speculative attacks which are capable of exploiting known vulnerabilities in critical systems, but which have never been perpetrated.[69] The above examples were selected to represent the unusual qualities that make cyberattacks difficult to place in the legal context of traditional notions of war, munitions, armed attack, and the use of aggressive force.

One characteristic of cyberattacks that is evident from these examples is civilian disruption. Whereas loss of life or physical destruction of property have occurred in only one known instance, Stuxnet, cyberattacks frequently disrupt civilian use of banking and media sources. Unfortunately, the impact of cyberattacks increases with the technological sophistication of the nation under attack. Estonian citizens, for example, conduct practically all of their banking transactions and access most of their government services over the Internet.[70] In cases in which attackers target more critical systems, such as power and water control mechanisms, the civilian impact is likely to be even greater; the twenty-four-hour-long power outage that occurred on the East coast of the United States in 2003 is a prime example of how software bugs can disrupt civilian life.[71]

Another characteristic is the difficulty of categorizing the effects of cyber-operations using classic descriptions of weaponry. How is a "cyber-weapon" classified when it has no physical manifestation other than inconvenience? How is data loss quantified? Assuming a nation has the right to counterattack, how do planners evaluate the proportionality of their response, especially if the counterattack includes traditional munitions?

68. *2012 Cyber Attacks Statistics*, HACKMAGEDDON.COM, http://hackmageddon.com/2012-cyber-attacks-statistics-master-index/ (last visited Apr. 26, 2013) (showing statistics and graphs on attack distribution in 2012).

69. *See, e.g.*, Dan Goodin, *Hacking Commercial Aircraft with an Android App (Some Conditions Apply)*, ARSTECHNICA (Apr. 11, 2103), http://arstechnica.com/security/2013/04/hacking-commercial-aircraft-with-an-android-app-some-conditions-apply/ (discussing vulnerabilities in the protocol used for sending data to commercial aircraft).

70. Davis, *supra* note 34.

71. *See* U.S.-CANADA POWER SYSTEM OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003 BLACKOUT IN THE UNITED STATES AND CANADA: CAUSES AND RECOMMENDATIONS (Apr. 2004), *available at* https://reports.energy.gov/BlackoutFinal-Web.pdf.

Another problem is in distinguishing the chosen method from the intended result. Cyber-operations can have unintended consequences.[72] For example, to keep its payload targeted at Iran and to lessen the chance of discovery, Stuxnet was designed not to be distributed over the Internet. However, it did spread to over 40,000 machines because of the unanticipated complexity of interconnected, non-internet networks.[73] Moreover, the methods of compromising a system for the purposes of espionage can be the same as that required for destructive damage. Since the intention of the attacker cannot be discovered purely by the method of the breach, it is more difficult to prioritize resources for defensive measures.

Perhaps the most atypical characteristic of cyberattacks, however, is the fact that they are often perpetrated by non-state actors.[74] Prosecutions under international law generally require a state actor. However, as the Georgian and Estonian incidents show, it is easy for a state to orchestrate the attacks—perhaps even providing the necessary tools to hackers sympathetic to the cause—then later deny involvement.[75] Attacks conducted by loosely affiliated groups in divergent geographical locations are not only difficult to defend against, but also extremely difficult to hold anyone accountable for later.[76] Further, even if a state instigates a cyberattack, it is often difficult to gather evidence of its involvement; the architecture of the Internet enables IP hiding and other forms of obfuscated attacks.[77] The servers that are used to perpetrate the attacks can be hidden in unassociated countries,[78] and attackers can even use compromised infrastructure belonging to unrelated parties to do their work.[79] These

72. *See* Stark, *supra* note 26.

73. *Id.*

74. *See* Bruce Schneier, *Understanding the Threats in Cyberspace*, SCHNEIER.COM (Oct. 28, 2013), https://www.schneier.com/blog/archives/2013/10/understanding_t_2.html.

75. *See, e.g.*, Anderson, *supra* note 31; Brenner, *supra* note 36.

76. *See, e.g.*, Anderson, *supra* note 31; Brenner, *supra* note 36.

77. *See, e.g.*, David B. Fein, *Coreflood Botnet Takedown & Civil Action*, U.S. DEPT. OF JUSTICE, http://www.justice.gov/usao/briefing_room/cc/mca_botnet.html (last visited Apr. 26, 2013); Dan Goodin, *Fueled by Super Botnets, DDoS Attacks Grow Meaner and Ever-More Powerful*, ARSTECHNICA (Apr. 17, 2013), http://arstechnica.com/security/2013/04/fueled-by-super-botnets-ddos-attacks-grow-meaner-and-ever-more-powerful/#p3n.

78. For example, it is likely that several of the botnets used in the Estonian DDoS attacks were located in the United States. *See* Fein, *supra* note 77.

79. Recently, vulnerable servers, usually the most powerful computers with the largest bandwidth connections to the Internet, have been increasingly compromised and used to create "super

characteristics of cyberattacks not only make it difficult to attribute the attack to any one party, but they also make traditional notions of territoriality under international law seem almost quaint.

IV. ACTS OF CYBER-AGGRESSION?

Article 8 *bis*, paragraph 2, defines an "act of aggression" as "the use of armed force by a state against the sovereignty, territorial integrity or political independence of another state."[80] It lists seven actions, lifted verbatim from Article 3 of U.N. G.A. Resolution 3314 (1974),[81] which conclusively qualify as acts of aggression. The constituents of this list are for the most part uncontroversial; they include such classic war maneuvers as the invasion, military occupation, or annexation by conventionally armed forces; naval bombardment and blockade; the sending of armed mercenaries; and a nation allowing its territory to be used as a launch point for another State to invade a third State.[82] As we have already seen, these classic notions of aggressive conduct fit poorly into the new modalities of aggression used in cyberattacks. Indeed, some commentators have wondered whether the definition is "already an anachronism."[83]

This reality hardly escaped the notice of the SWGCA or the States Parties at Kampala,[84] but how broadly did the negotiating parties intend the ICC to construe this list of aggressive acts? The negotiation history shows that even the parties themselves understood the answer to this question to be ambiguous.[85] This ambiguity stems from three sources. The first is the problem with reconciling an open-ended understanding of illegal acts with the principle of legality. The second is the difficulty in using G.A. Resolution 3314, aimed at establishing *state* liability for aggressive behavior, as a definition for an individual crime in a court set up for *jus in bello* prosecutions.[86] The third source is political and reflects the tension

botnets" that can cause far greater disruption than mere desktops. *See* Goodin, *Fueled by Super Botnets*, *supra* note 77.

80. Rome Statute, *supra* note 6, at art. 8 *bis*, para. 2.

81. G.A. Res. 3314 (XXIX), U.N. Doc A/RES/3314 (Dec. 14, 1974) [hereinafter Res. 3314].

82. Rome Statute, *supra* note 6, para. 2(a)–(g).

83. *See, e.g.*, Noah Weisbord, *Conceptualizing Aggression*, 20 DUKE J. COMP. & INT'L L. 1, 22 (2009).

84. *See* Weisbord, *Judging Aggression*, *supra* note 1, at 99.

85. *See* Barriga, *supra* note 3, at 24.

86. *See id.* at 25.

between the interests of aligned states, non-aligned states, and the permanent members of the U.N. Security Council. All of these factors shaped a solution that allows each negotiating party to view an act of aggression through the prism of its own presuppositions. Ultimately, however, the compromise delegates substantial discretion both to the U.N. Security Council and to the ICC judges.

From September 2005, when discussions about the meaning of an act of aggression began in earnest, the members of the SWGCA grappled with whether to craft a generic definition or a specific one.[87] Certain parties, including those on the Security Council, favored a specific approach using Resolution 3314 because it allowed the Security Council to be the ultimate authority in labeling an act of aggression.[88] Other parties, like Greece and Portugal, recognized that it was not possible to create a specific, but still comprehensive, list of aggressive acts.[89] Therefore, in their view, any such list would violate the principle of legality because it would need to be interpreted, which would not sufficiently notify the accused of the criminality of their acts.[90] Consequently, these parties favored a generic approach that outlawed any illegal use of force aimed at the sovereignty of a state.[91] Eventually, the stalemate was broken in 2007 when early proponents of the generic approach agreed to yield their position.[92]

The task then turned to adapting Resolution 3314, a non-binding resolution from 1974 aimed at circumscribing the limits of *jus ad bellum*.[93] This was problematic not only because it had to be adapted to prosecute individuals, rather than States, for aggression, but also because here, too, the principle of legality must be satisfied. The primary sticking points were neither in the list of acts in Article 3, nor in the chapeau provisions of Article 1 of Resolution 3314. Instead, the problem was with Article 4, which reads, "The acts enumerated above are not exhaustive and the Security Council may determine that other acts constitute aggression under

87. *See id.* at 24.
88. *Id.* at 25.
89. *Id.*
90. *Id.*
91. *Id.* Within the "generic approach" camp, however, Germany favored an extremely high threshold including only annexation or occupation. *Id.*
92. *Id.*
93. Res. 3314, *supra* note 81.

the provisions of the Charter."[94] Many parties felt that leaving the definition of aggression to the future discretion of the U.N. Security Council, an international body unrelated to the ICC, would violate the principle of legality, and so Article 4 of Resolution 3314 could not be incorporated whole-cloth.[95] The drafters ultimately decided to leave Article 4 out, but as will be seen below, it is still an open question whether Article 4 will continue to influence the interpretation of the definition.

On the other hand, the negotiators still felt the need to make the crime of aggression relevant and adaptable to unforeseen future scenarios. A 2007 proposal by Venezuela attempted to widen the notion of aggression with two additional subsections to Article 8 *bis* paragraph 2.[96] These new subsections would incorporate into the list of prohibited acts financial and commercial restrictions (new subsection "h") and "any other form of attack which, without involving the use of armed force, violates the . . . territorial integrity . . . of [a] State[]" (new subsection "i").[97] While this proposal had the advantage of expanding the traditional notion of aggression, thus clearly incorporating cyberattacks into the definition without delegating the question to an outside body, it received little discussion.[98] Most likely, this proposal was considered too open-ended and parties viewed the language in the new subsection "i" ("without . . . armed force") as too difficult to merge with the language of Resolution 3314.

All in all, it seems clear that the list of acts in Article 8 *bis* paragraph 2 was not intended to be a closed list. The first and simplest reason is semantic: if the drafters had meant to limit the list, the easiest way would have been to use the phrasing "only the following acts" rather than "any." Second, the negotiation history shows that the parties considered the principle of legality to be the primary reason to keep the list narrow; the reason for a narrow list was not merely the political desire to make more

94. *Id.* at art. 4.

95. *Report of the Special Working Group on the Crime of Aggression*, ICC-ASP/6/SWGCA/1, *in ASP Official Records*, ICC-ASP/6/20, Annex II, 87, para. 21 [hereinafter *December 2007 SWGCA Report*].

96. *Id.*

97. *Revised Text of the Proposal Submitted by the Bolivarian Republic of Venezuela on the Question of the Definition of the Crime of Aggression and Conditions for the Exercise of Jurisdiction*, 7 Dec. 2007, ICC-ASP/6/SWGCA/WP.1 [hereinafter *2007 Venezuela Proposal*].

98. *See* Assembly of States Parties, June 2–6, 2008, *Report of the Special Working Group on the Crime of Aggression*, U.N. Doc. ICC-ASP/6/20/Add.1, para. 35 (2008), (2008) [hereinafter *June 2008 SWGCA Report*].

types of conduct permissible. Indeed, the June 2008 SWGCA Report declared "the right balance had been struck . . . by including a generic definition in the chapeau of paragraph 2, along with the non-exhaustive listing of acts of aggression."[99]

The fact that the list was meant to remain open to interpretation, at least to an extent, begs the question: how broadly may the ICC construe acts of aggression? Several interpretations are possible, partly depending on the how the ICC assays the Article 8 *bis* paragraph 2 language "in accordance with United Nations General Assembly Resolution 3314." On one hand, ICC judges may interpret this to mean "in accordance" with the *entirety* of Resolution 3314, which would include the omitted Article 4 and its intent to defer to the U.N. Security Council any extension of the acts of aggression beyond the enumerated list. Under this reading, the ICC would wait for the U.N. Security Council to rule on any acts of aggression that did not strictly fit into the enumerated categories, either by ruling an *actual act by a state* as aggression under its Article 15 *bis*, paragraph 6 powers, or by using its Resolution 3314 Article 4 power to amend or broaden the list defining an aggressive act.[100]

However, it is unnecessary for the ICC to feel unduly restricted by the "in accordance" language, at least in any legal sense. First, the negotiation history does not lend itself to the idea that the negotiators wished to re-bind themselves to the U.N. Security Council after explicitly deciding not to include Article 4 of Resolution 3314 in the new Article 8 *bis*.[101] Second, the syntactic placement of the modifier "in accordance with" does not imply that it was intended to enforce strict adherence to Resolution 3314, but only that the negotiators desired to reference that resolution because the subsequent list of acts was taken verbatim from it. In fact, the negotiators' explicit intent was to reference Resolution 3314 because it established credibility and because doing so would build consensus between the States Parties—not to imply that the ICC would be bound by it.[102] Third, such a reading would contravene the purposes of the "without prejudice" clauses

99. *Id.* at para. 34.
100. *See* Weisbord, *Judging Aggression*, *supra* note 1, at 40; Barriga, *supra* note 3, at 26.
101. *December 2007 SWGCA Report*, *supra* note 95, para. 20–21.
102. *See* Barriga, *supra* note 3, at 27.

in Article 15 *bis* paragraph 9 and Article 15 *ter* paragraph 4,[103] both of which are specifically present to ensure that the ICC is not beholden to potentially politically motivated U.N. Security Council determinations of aggressive acts.[104]

If the ICC indeed has the authority to widen the notion of an act of aggression, what method of interpretation should it use to do so? Accepting that the list is open, not strict, allows jurists to use the acts in Article 8 *bis*, paragraphs 2, subparagraphs (a) through (g) as analogical, interpretive examples that clarify the types of acts that the parties intended to prohibit. Essential to that effort, however, is that jurists read broadly the chapeau's notion of "use of armed force."[105] Without also expanding the traditional understanding of "armed force," extending the Article 8 *bis* paragraph 2 list by analogy is simply insufficient.

It is instructive to begin with a few concrete analogies. In this way, jurists can explore similarities in methods or effects between classic examples of aggression and acts of cyber-aggression. For example, Article 8 *bis* paragraph 2, subparagraph (a) refers to "an invasion . . . of the territory of another state, or any military occupation, however temporary, resulting from such invasion."[106] Analogizing from this, one state's installation of a computer virus on the military networks of another state, causing it to "temporarily occupy" the state's territory (its memory chips and computer hard drives), could be understood to violate this prohibition.[107] A state could also violate paragraph 2, subparagraph (a) by "annexing" a nation's computer networks to create a botnet to attack some other state. A further example: Article 8 *bis* paragraph 2, subparagraph (c) prohibits "blockade" by a State. Traditionally this would be understood as a naval blockade against a nation's ports or coasts, but a denial-of-service cyberattack, as perpetrated against Georgia, can work similarly. If the

103. Both paragraphs are identical and read, "A determination of an act of aggression by an organ outside the Court shall be without prejudice to the Court's own findings under this Statute." Rome Statute, *supra* note 6, art. 15 *bis*, para. 9, art. 15 *ter*, para. 4.

104. *See* Claus Kress & Leonie von Holtzendorff, *Kampala Compromise on the Crime of Aggression*, 8 J. INT'L CRIM. JUST. 1179, 1194 (2010).

105. Rome Statute, *supra* note 6, art. 8 *bis*, para. 2.

106. Kampala Compromise, *supra* note 12, at art. 8 bis, para. 2(a).

107. If this seems farfetched, consider that many notions in copyright law hinge on whether a temporary copy of a software program in RAM is a "copy" for the purposes of the Copyright Act. *See* MAI Systems v. Peak Computer Corp., 991 F.2d 511 (9th Cir. 1993).

DDoS attack disrupted communications to such an extent that vital connections to the outside world were severed, it would have similar effects to a blockade and therefore might be considered a violation of Article 8 *bis* paragraph 2, subparagraph (c). Finally, consider Article 8 *bis* paragraph 2, subparagraph (f), which prohibits a state from allowing a second state to use its territory as a platform from which to aggress against a third state. Hypothetically, if China allows or knowingly tolerates North Korea's use of its computer networks to stage a cyberattack against South Korea, it might be violating subparagraph (f). Such analogies are limited only by the imagination.

At the outset, it is important to note the explicit prohibition, which is found in Article 22, paragraph 2 of the Rome Statute, against extending the literal definition of a crime by analogy.[108] This proscription would be very problematic if the Kampala Compromise Article 8 *bis* paragraph 2 were the full and complete description of the elements of the crime of aggression. Under an open interpretation, however, the acts listed in Article 8 *bis* paragraph 2 are definitive, explicit *examples* of an "act of aggression." If those acts *also* meet the other conditions in the chapeau,[109] they constitute one element of the "crime of aggression." Thus, under the understanding of the relationship between the chapeau in Article 8 *bis* paragraph 1 and the list in Article 8 *bis* paragraph 2 developed above, using analogy to understand the characteristics of a cyberattack does not violate Article 22, paragraph 2 of the Rome Charter because the list of acts in Article 8 *bis* paragraph 2 are not traditional "elements" of the crime.[110]

The examples above, in addition to stretching analogy somewhat beyond the "manifest violation" requirement, have a second difficulty: analogies have limits. Even with a fertile imagination, some methods of cyberattack simply have no analogue in the conceived list of aggressive acts from 1974. For example, manipulating a country's financial markets

108. Article 22, paragraph 2 states, in pertinent part: "The definition of a crime shall be strictly construed and shall not be extended by analogy. In case of ambiguity, the definition shall be interpreted in favour of the person being investigated, prosecuted or convicted." Rome Statute, *supra* note 6, art. 22, para. 2.

109. The negotiation history shows that the Parties understood that even acts in Article 8 *bis* (2) had to meet the threshold requirements of character, gravity, and scale in Article 8 *bis* (1). Barriga, *supra* note 3, at 28–30.

110. *But cf.* Weisbord, *Judging Aggression*, *supra* note 1, at 40 (taking a firmer position that the use of analogy is prohibited under Article 22, paragraph 2).

with a Trojan horse or the hack of a Twitter account is neither an attack on its "armed forces" nor a use of armed force in a strict sense. Without a broader understanding of armed force beyond its explicit meaning, such analogies can be applied only to attacks by military forces on military targets. Some, but certainly not all, of the cyberattacks in Part III, *supra*, meet these restrictions. However, merely extending the list of crimes by analogy is insufficient without concomitantly expanding the notion of armed force beyond its traditional boundaries.

The negotiation history can help to clarify the contours of "armed force" in a cyber-aggression context. At the time of the January 2007 SWGCA Report, language referring to "act of aggression" and "armed attack" was still present in draft proposals and still under debate.[111] By the time of the June Princeton Report, the negotiators had agreed that "armed attack" would be removed in favor of the familiar Resolution 3314, Article 2 language, which prefers the term "armed force" to set the boundaries of aggression.[112] Since Resolution 3314 is a U.N. Resolution, the meaning of armed force must be interpreted in the context of the U.N. Charter's understanding of that term. In addition, to reinforce the importance of this interpretation, the negotiators required that the use of force be "inconsistent with the Charter of the United Nations."[113]

A more expansive understanding of armed force allows the ICC to view "armed" as meaning all forms of military-sponsored or state-sponsored uses of force. So long as the intent is aggressive and satisfies the threshold clause so as to violate the U.N. Charter, the physical characteristics of the putative armament matter little. "Force" is also a more capacious term than "attack," allowing the ICC to incorporate the substantial body of criticism involving the "use of force" that exists to interpret Article 2, paragraph 4[114] and Article 51[115] of the U.N. Charter. A

111. *Report of the Special Working Group on the Crime of Aggression*, ICC-ASP/5/SWGCA/2 (Jan. 2007), *in ASP Official Records*, ICC-ASP/5/35, Annex II, 9, para. 14 [hereinafter *January 2007 SWGCA Report*].

112. *Informal Intersessional Meeting of the Crime of Aggression, held at the Liechtenstein Institute on Self-Determination, Woodrow Wilson School, Princeton University, United States, from 11 to 14 June 2007*, ICC-ASP/6/SWGCA/INF.1, *in ASP Official Records*, ICC-ASP/6/20, Annex III, 96, para. 51 [hereinafter *2007 Princeton Report*].

113. Rome Statute, *supra* note 6, art. 8 *bis*, para. 2.

114. Article 2(4) states, in pertinent part, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state . . . ." U.N. Charter art. 2, para. 4.

full account of *jus ad bellum* rules with regard to the use of force is beyond the scope of this Article, but, as will be discussed in Part VI, *infra*, certain kinds of cyberattacks do qualify as uses of armed force under the UN Charter, at least according to recent NATO and U.S. interpretations.[116]

Ultimately, political realities may trump any legal argument as a basis for the ICC's independence in widening the notion of aggression to include cyber-aggression. As will be seen, it may be that the ICC is hamstrung by procedural safeguards and *realpolitik*, requiring it to defer to the U.N. Security Council as a practical matter, regardless of the legal standing it has to make its own interpretation.

V. THE "THRESHOLD" OF CYBER-AGGRESSION

To rise to the level of aggression, a cyberattack must also meet the "threshold" requirements.[117] This distinct, yet highly intertwined, element is that the act of aggression be a "manifest violation" of sufficient "character, gravity, and scale."[118] These modifiers, along with Understandings 6–7 of Resolution RC/Res.6, form the *de minimis* threshold to which any act of aggression must rise before the ICC will act. The threshold element is intended to confine the crime of aggression to the most serious violations of international law.

The negotiators in the SWGCA considered several alternatives before settling on "manifest," including "serious" and "flagrant."[119] By mid-2006, however, the parties had decided on "manifest"[120] primarily because the term had a more settled understanding in international law. "Manifest" has a well-understood, objective connotation,[121] while it was feared that

115. Article 51 gives a nation the right of self-defense, regardless of U.N. resolution: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member . . . ." U.N. Charter art. 51.

116. *See* Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARV. INT'L. L.J. ONLINE 13, 18–20 (2012).

117. *See* Rome Statute, *supra* note 6, art. 8 *bis*, para. 1.

118. *Id.* This paragraph is also termed the "threshold clause."

119. Barriga, *supra* note 3, at 28–29.

120. *Informal Intersessional Meeting of the Crime of Aggression, Held at the Liechtenstein Institute on Self-Determination, Woodrow Wilson School, Princeton University, United States, from 8 to 11 June 2006*, ICC-ASP/5/SWGCA/INF.1, *in ASP Official Records*, ICC-ASP/5/32, Annex II, 387, para. 20 [hereinafter *2006 Princeton Report*].

121. *See, e.g.*, Article 46(2) of the Vienna Convention on Treaties.

"flagrant" would be too subjective.[122] Indeed, the objectiveness of "manifest" was so important to the parties that they reinforced the concept in the Amendments to the Elements of Crimes.[123] Further, the negotiation history shows the threshold clause, part of the chapeau in Article 8 *bis* paragraph 1, must be interpreted as a limitation on the acts of aggression described in Article 8 *bis* paragraph 2, intended to exclude controversial applications of the use of force.[124] However, this understanding was itself contentious. The parties who favored the threshold clause argued that it was necessary to ensure that the ICC did not become bogged down in "borderline cases" and would consider only the most serious violations.[125] However, certain of the non-aligned delegations, notably Egypt and Iran, felt that the threshold clause undermined the power of G.A. Resolution 3314 because it amounted to a second standard that an act of aggression would be required to meet—in contravention of the explicit examples in Art. 8 *bis* paragraph 2.[126] Other parties also argued that the additional, limiting qualifier was unnecessary because it was inherent in Article 1 of the Rome Statute[127] that the Court would only concern itself with the most serious international crimes.[128] Ultimately, however, the inclusion of the threshold clause turned out to be essential to reaching consensus on the inclusion of G.A. Resolution 3314 because the threshold clause allowed those delegations who feared an overly specific definition to foresee at least the possibility that acts other than those listed might be subject to prosecution.[129]

If "manifest" implies an objective standard, what do the additional attributes "character, gravity, and scale" signify, as applied to an act of aggression? Each of these attributes help to portray the severity of an act of

122. Barriga, *supra* note 3, at 29 n.146.

123. Kampala Compromise, *supra* note 12, ann. II, para. 3 ("The term 'manifest' is an objective qualification.").

124. *See* BASSIOUNI, *supra* note 2, at 669.

125. *2006 Princeton Report*, *supra* note 120, para. 19. *See also id.* para. 16. ("I believe that a high threshold, as expressed by the term 'manifest,' to be understood objectively, and the combined existence of character, gravity and scale . . . is necessary to stress the difference between the act and crime of aggression and to avoid its trivialization.").

126. *December 2007 SWGCA Report*, *supra* note 95, para. 13.

127. Rome Statute, *supra* note 6, art. 1 states, in pertinent part, that the ICC ". . . shall have the power to exercise its jurisdiction over persons for the most serious crimes of international concern . . . ."

128. *2006 Princeton Report*, *supra* note 120, para. 18.

129. *2007 Princeton Report*, *supra* note 112, para. 48.

aggression in terms of three facets: effort, effects, and intention, respectively. "Scale" refers to the size of the attack, as in the number of resources mobilized and the level of planning and coordination needed to achieve the effort. A small team invading a compound in Pakistan to capture a suspected terrorist, for example, might not rise to the appropriate scale because only a small number of resources were used. In like manner, the word "gravity" suggests the extent of the consequences of an attack: the fact that the attack results in human deaths, for example, rather than property damage. "Character," on the other hand, is more difficult to conceptualize because it possesses a hint of subjectivity. It is important to note, however, that the character of an act is not evaluated from the purely subjective viewpoint of the aggressor; it will be evaluated by the ICC according to objective standards.[130] Even so, such an evaluation must be, to some degree, a matter of the perspective of the evaluator.[131] The people ordering the act of aggression on behalf of their state may believe their motives are humanitarian—and many other nation-states may agree—but that does not mean other nations with different humanitarian or geopolitical perspectives also agree that the act's character was benign. The ICC is then faced with the task of deciding whose perspective most aligns with international consensus.

A matter of some contention during the negotiations was the relative weight that the ICC should give these factors in considering whether a violation is manifest. During the two weeks of the Kampala Review Conference, the U.S. voiced several concerns[132] about the meaning of "character, gravity, and scale," and proposed two new "understandings" to mitigate them.[133] The major concern was that it was unclear how the ICC would weigh these factors in its determinations. Thus, it was unclear

130. Andreas Paulus, *Second Thoughts on the Crime of Aggression*, 20 EUR. J. INT'L L. 1117, 1121 (2009).

131. *See id.*

132. Harold Koh, *Statement at the Review Conference of the International Criminal Court*, U.S. DEP'T OF STATE WEBSITE (June 4, 2010), http://www.state.gov/s/l/releases/remarks/142665.htm [hereinafter *Koh Kampala Statement*].

133. Claus Kress et al., *Negotiating the Understandings on the Crime of Aggression*, *in* THE TRAVAUX PRÉPARATOIRES OF THE CRIME OF AGGRESSION 81, 94–95 (Stefan Barriga & Claus Kress eds., 2012). Note that, while the U.S. is not a party to the Rome Charter, its delegation was accommodated by the negotiators because they believed engaging with the U.S. would be helpful later, when U.N. Security Council support was needed to help prosecute aggressors. Kress & von Holtzendorff, *supra* note 104, at 1205.

whether situations might arise in which one factor, such as "scale," was so massively overweighed that the "character" of the act might be forgotten. The German and Canadian delegations also submitted proposals on these topics;[134] this combined effort eventually produced Understandings 6 and 7, which had the effect of clarifying that the ICC would conduct a totality-of-the-circumstances evaluation as to all three factors and that no one factor would be so heavily weighed as to overshadow the insufficiency of the other two factors.[135]

The true weight of these factors, each of which will be required to exhibit a "manifest" violation is, as yet, unknown. One consideration is that the two different methods of referral to the ICC may end up resulting in two different standards for character, gravity, and scale: a lighter standard which is applied to States Parties who have not opted out and a much heavier standard for non-parties (whose conduct has to rise to the rare level which prompts U.N. Security Council unanimity).[136] Andreas Paulus, for example, opines that the "character" limitation may be sufficient to knock down any level of gravity and scale in the use of force.[137] Indeed, Claus Kress, prominent scholar of the crime of aggression and member of the German delegation, has stated that the 2003 Iraq War was not aggression[138] and that "only a 'war of conquest and hegemonial war' constitute historical precedents for a war of aggression."[139]

A final consideration is the link between the "manifest" act of aggression and the mental state of the individual perpetrator. Element 6 of the crime of aggression requires the perpetrator to be "aware of the factual circumstances that established such a manifest violation."[140] This element echoes the general *mens rea* requirements of Article 30 of the Rome

134. Kress et al., *supra* note 133, at 96.

135. Kampala Compromise, *supra* note 12, ann. III, para. 6–7.

136. Weisbord, *Judging Aggression*, *supra* note 1, at 100 ("Since the Council began its work in 1945, it has only made express resolutions condemning aggression thirty-one times. Meanwhile, a recent study concluded that 313 armed conflicts took place between 1945 and 2008.").

137. Paulus, *supra* note 130, at 1123. *Contra* Kress & von Holtzendorff, *supra* note 104, at 1207 (arguing that the "sliding scale" problem arises only with respect to gravity and scale, and that the "character" factor resolves, rather than exacerbates, any gray areas).

138. Paulus, *supra* note 130, at 1123.

139. *Id.* at 1122.

140. Kampala Compromise, *supra* note 12, ann. II, para. 6.

Statute, which requires both intent and knowledge.[141] Read together, these provisions limit culpability in the expected way. For example, a group perpetrating a small cyberattack on a bank would not be a part of a larger, manifest act of aggression if they were unaware that government groups were conducting a more concerted effort against military targets at the same time.[142] The DDoS attacks on Georgia, if indeed they were perpetrated by nationalists who did not know of Russia's plans for a traditional attack, might also fail on *mens rea*, assuming the DDoS attacks in and of themselves were not sufficiently aggressive.

In other examples of cyberattacks, it is more difficult to understand whether *mens rea* would be satisfied, particularly in cases where certain conduct and consequences might be intended but other consequences that are clearly "possible in the ordinary course of events" occur instead. Stuxnet, for example, was propagated much more widely than its intended target of Iranian nuclear centrifuges, but since it was only intended to affect computers containing PLC controller software, it had no lasting deleterious effects on other infected machines.[143] However, had Stuxnet somehow caused unintended damage—such as a chain reaction of nuclear material in the centrifuges (very implausible), or some effect on oil pipeline control software or power grid software once it spread to machines using the same Siemens development tools (much more plausible)—would the individuals be liable for the unintended, yet perhaps foreseeable, consequences of their action? It remains to be seen whether an unintended, yet foreseeable, consequence which greatly amplifies one factor (in this case, "gravity") might push an act of aggression over the limit to "manifest."

In addition, Paragraphs 2 to 4 of the Introduction to the Elements[144] clarify that a mistake-of-law defense as to the threshold clause is not available to perpetrators. No legal evaluation that the perpetrators conducted on their own behalf, or failed to conduct, will absolve them of culpability if the ICC finds that the act was sufficiently aggressive. This

141. Rome Statute, *supra* note 6, art. 30. ("'[K]nowledge' means awareness that a circumstance exists or a consequence will occur in the ordinary course of events.").

142. *See* Frances Anggadi et al., *Negotiating the Elements of the Crime of Aggression*, *in* THE TRAVAUX PRÉPARATOIRES OF THE CRIME OF AGGRESSION 58, 75–76 (Stefan Barriga & Claus Kress eds., 2012). Note that this illustrative example does not even touch upon the other ways in which such an attack would *not* be a crime of aggression, i.e., state action.

143. *See supra* Part III.A.

144. Kampala Compromise, *supra* note 12, ann. II, Introduction, para. 2–4.

helps to mitigate concerns that, in an era of secret government memoranda that justify behaviors ranging from torture to drone attacks, rationalizations about the "character" of a perpetrator's intention can only go so far.[145] More specifically, these provisos establish an important principle in the area of cyberattacks because the legal status of cyber-aggression is completely unsettled in international law.

From the preceding discussion, four primary interpretive principles emerge in relation to acts of aggression. One, ICC judges have some latitude in interpreting what kinds of acts use armed force because the list of acts in Article 8 *bis* paragraph 2 is not exhaustive. Two, the words "armed force" can and should be interpreted in light of *jus ad bellum* jurisprudence stemming from Article 2(4) and Article 51 of the U.N. Charter. Three, the ICC must assess whether any act of aggression using armed force is "manifest" by assessing the sum of three measures: the character of its intent, the gravity of its effects, and the scale of its methods. Four, "manifest" is an objective measure, irrespective of the opinion of the perpetrator. Now we turn to the question of whether international standards and state practice can impact the interpretation of these fairly flexible interpretive principles.

VI. IMPACT OF STANDARDS AND STATE PRACTICE ON THE "THRESHOLD" OF CYBER-AGGRESSION

Recent developments suggest that international diplomacy, standard-setting, statecraft, rhetoric, and national saber-rattling may be more relevant to adjudicating whether an act of aggression meets the threshold standard than it seems at first blush. There are two reasons for this. First, such activities establish that the perpetrators knew the given conduct would meet the threshold clause, as Elements 4 and 6 require. For example, say a nation "saber-rattles" by warning a second nation that a certain act could trigger the first nation to invoke its right to self-defense with a certain response.[146] If the first nation later does attack in "self-defense," but the second nation's act did not truly rise to a level justifying self-defense, the first nation can hardly feign ignorance of the factual circumstances of its

145. *See* Paulus, *supra* note 130, at 1123.

146. I.e., the act rises to the level of an "armed attack" under Article 51 of the U.N. Charter.

attack.[147] A second and more subtle point, though, is that standard-setting and rhetoric have a propagandizing effect, alerting the world to the character of certain actions and encouraging normalization and consensus. Indeed, over time, this is how customary international law is created.[148] It is to this second point that we now turn.

A. IMPACT OF INTERNATIONAL STANDARDS

One standard-setting effort that is poised to have a major impact on the international understanding of cyber-operations is the *Tallinn Manual*.[149] The work is the product of a three-year effort by an "international group of experts" commissioned by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, to examine the applicability of international norms in *jus ad bellum* and *jus in bello* to cyber-warfare.[150] The *Tallinn Manual* is not an official NATO document, nor does it necessarily represent the views of NATO's member nations.[151] However, many of the experts are renowned scholars.

At the outset, it is important to re-emphasize that the *Tallinn Manual*'s focus is on defining the limits of cyber-aggression from the perspective of the U.N. Charter, specifically Articles 2(4) and 51. As noted earlier, however, the ICC may analyze the meanings of "use of force," "armed force," and "armed attack" through the lens of those Articles because of the added proviso that, to be a crime, the use of force must be "in a manner inconsistent with the Charter of the United Nations."[152] In fact, a major condition of the new definition demands that the U.N. Security Council have the opportunity to classify a State's act as aggression before the ICC can proceed with its investigation.[153] Thus, not only is reading aggression

147. This is not the same as requiring the first nation to have "made a legal evaluation," which is specifically precluded by the elements. Kampala Compromise, *supra* note 12, ann. II, Introduction, para. 2–4. This "rhetoric" establishes that the first nation admitted it had cyber-weapons of a certain character and intended to use them. *Id*.

148. *See* RONALD C. SLYE & BETH VAN SCHAACK, INTERNATIONAL CRIMINAL LAW: THE ESSENTIALS 95–97 (2009).

149. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN].

150. *The Tallinn Manual*, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE WEBSITE, http://www.ccdcoe.org/249.html (last visited Apr. 16, 2013).

151. *Id.*

152. Rome Statute, *supra* note 6, art. 8 *bis*, para. 2.

153. *Id.* art. 15 *bis*, para. 6–8.

in the light of traditional *jus ad bellum* analysis possible, the interpretive and jurisdictional restraints on the crime of aggression practically require such a reading.

At this juncture, a few words about the relationship of the crime of aggression to customary international law are appropriate. During Kampala, the U.S. delegation voiced concerns that the list of acts drawn from G.A. Resolution 3314 would not, in all cases, align with customary international law. The delegation therefore proposed an understanding which would explicitly dissociate the two, stating that it "shall not be interpreted as constituting a statement of the definition . . . under customary international law."[154] The U.S. felt that the crime of aggression was much less developed at that time than the crimes of genocide, war crimes, and crimes against humanity were when defined by the Rome Charter. Apparently in response to this, the U.S. wanted to ensure that the future development of customary international law regarding aggression would not be impacted by the ICC's definition.[155] As a non-party to the Rome Statute, the U.S. may not have wanted any obligations that it had under customary international law to be burdened by a definition created without its participation. It is also possible that the U.S. realized the significance of its own saber-rattling and practices on the international understanding of aggression, a point which will be made more expansively below. However, the actual reasons for the U.S. position are unknown. As it turns out, other delegations were adamantly opposed to the U.S. position, and the references to customary international law were dropped from what eventually became Understanding 4.[156]

If *Tallinn* is indeed of valid interpretive use, then what does it have to say about the key notions of "armed force," "act of aggression," and "manifest" that might be useful in understanding the crime of aggression? According to *Tallinn*, international law is relatively unambiguous with regard to the means employed:

> The International Court of Justice has stated that Articles 2(4) [and] 51 . . . apply to "any use of force, regardless of the weapons employed." The [experts] unanimously agreed that this statement is an accurate reflection of

154. Kress et al., *supra* note 133, at 93.
155. *Id.* at 92.
156. *Id.* at 93.

> customary international law. . . . The mere fact that a computer . . . is used . . . has no bearing on whether that operation amounts to a "use of force."[157]

Furthermore, using *jus ad bellum* principles to analyze the pertinent thresholds of "scale and effects" can lend valuable clarity to the similar terms "character, gravity, and scale" under the crime of aggression.[158] The *Tallinn Manual*'s Rule 11 discusses the factors influencing what kinds of actions short of an armed attack are still a "use of force."[159] Acts injuring or killing persons or destroying objects are clearly uses of force, but other types of acts may not be. The Tallinn experts advise, "States contemplating cyber operations, or that are the target thereof, must be highly sensitive to the international community's probable assessment of whether the operations violate the prohibition on the use of force."[160] Thus, an essential part of the analysis is to consider what *other states* would think about the cyber-operation.

To carry out this analysis, *Tallinn* proposes an eight-factor test which is not necessarily all-inclusive: (1) severity, (2) immediacy, (3) directness, (4) invasiveness, (5) measurability of effects, (6) military character, (7) state involvement, and (8) presumptive legality.[161] Of these factors, severity likely carries the most weight because physical damage to property or harm to individuals will always be considered a use of force, trumping the other concerns.[162] However, cyber-operations produce a wide variety of effects in the vast gray area between physical harm and inconvenience. The more that nations view a cyber-operation as impacting a vital national system or interest, the more likely the severity threshold will be met. Duration and intensity would also be considered.[163] It is an interesting consequence, however, that under this rubric the severity bar is continually lowered as societies advance technologically.[164] In fact, severity may be

157. TALLINN, *supra* note 149, at 42.
158. *See id.* at 48.
159. *Id.*
160. *Id.*
161. *Id.* at 48–51. *See also* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 845–49 (2012).
162. TALLINN, *supra* note 149, at 48.
163. *Id.*
164. TOURÉ, *infra* note 240, at 89–90.

evaluated differently depending on a given nation's degree of technological development.[165]

The question of severity is more difficult to evaluate in situations where vital property was destroyed, but the property is intellectual rather than physical. It is at this juncture that the other factors become more relevant in the analysis. For example, the Shamoon attack on Saudi Aramco wiped the hard drives of many thousands of computers at that company. Under the fifth factor, measurability of effects, a virus that had specific and quantifiable damage would be more likely to be viewed as an act of force than one which had a negligible effect on productivity or a few days of down-time.[166] Shamoon, then, would rank highly under this test. Further, the directness factor assesses the causal strength of the link between the intent of a cyber-operation and its effects.[167] An attack that erased data intentionally, as Shamoon did, rather than as a side effect or unintended consequence, would score higher here. Under the invasiveness factor, penetrations into more highly secured systems are more likely to be uses of force, and penetrations of military systems factor more highly than do penetrations of civilian systems.[168] Stuxnet, which penetrated into Iran's most highly guarded nuclear production systems, would score very highly on the invasiveness scale, whereas Anonymous' hacking of the public U.S. Department of Justice website would score much lower. In addition, acts that can be attributed directly to a nation's military units (factor six) carry more weight than those perpetrated by unknown parties or loosely affiliated nationalist groups.[169] Even in situations where a non-state group perpetrates the cyber-operation, the closer the group is to state sponsorship, tolerance, or state-provided safe harbor (factor seven), the closer the act comes to a use of force.[170] Last, but not least, acts that are *not prohibited* by international treaty or custom (factor eight), or which are widely

165. Thus, double standards are likely to persist here, as in other areas of international law. For example, a telephone network attack against an African nation might not be considered a use of force because it does not affect a widely used, vital system. The same attack against Canada might be considered a use of force, however.

166. TALLINN, *supra* note 149, at 50.

167. *Id.*

168. *Id.* at 49.

169. *Id.* at 50–51.

170. *See id.* at 51.

tolerated—such as state-to-state espionage, propaganda, or economic pressure—are less likely to be considered uses of force.[171]

Under the *Nicaragua* judgment, the International Court of Justice made a distinction between the mere use of force and "the most grave forms of the use of force."[172] These latter uses of force may cross a threshold that makes them an "armed attack" by virtue of their scale and effects.[173] Evaluation of the scale and effects of a use of force to see if it rises to the level of "armed attack" is conducted using the same eight-factor test discussed earlier. Some cases of cyberattacks are relatively simple to categorize: "The clearest cases are those cyber operations, such as the employment of the Stuxnet worm, that amount to a use of force."[174] Some of the experts even felt that Stuxnet had reached the "armed attack" threshold, unless of course it was justified on the basis of anticipatory self-defense.[175] On the other hand, the international community, officials of Estonia, and the panel of *Tallinn* experts did not think that the 2007 DDoS attacks against Estonia rose to the level of an "armed attack" justifying a self-defensive counterattack.[176] To summarize *Tallinn*, "Some cyber actions are undeniably not uses of force, uses of force need not involve a State's direct use of armed force, and all armed attacks are uses of force."[177]

Such categorizations are important because, under the U.N. Charter, a state may legally use force to defend itself once it has suffered an "armed attack,"[178] or once an attack has clearly been launched but has not yet reached its destination. In addition, despite the early arguments of one commentator that an exception for self-defensive action may not be permitted under a literal reading of the crime of aggression proposed just

171. *Id.*

172. Nicaragua v. United States, I.C.J. ¶ 191 (June 27, 1986), *available at* http://www.icj-cij.org/docket/files/70/6503.pdf.

173. TALLINN, *supra* note 149, at 47.

174. *Id.* at 45. *See also* Kim Zetter, *NATO Researchers: Stuxnet Attack on Iran Was Illegal "Act of Force"* WIRED (Mar. 25, 2013), http://www.wired.com/threatlevel/2013/03/stuxnet-act-of-force/.

175. TALLINN, *supra* note 149, at 58.

176. *Id.* at 57–58.

177. *Id.* at 47–78.

178. U.N. Charter art. 51.

prior to Kampala,[179] under the interpretation of most commentators, a self-defensive act does not amount to a crime.[180]

Self-defensive actions which occur *before* any attack has occurred are called "anticipatory self-defense."[181] Such actions are permissible under international law but are severely constrained.[182] The *Tallinn Manual*'s Rule 15 deals with the circumstances under which anticipatory self-defense is permitted.[183] The "imminence" of the attack is the key consideration.[184] Under the prevailing standard for imminence, the "last feasible window of opportunity" standard, a state's ability to preemptively defend begins only at the last moment when the nation *could have* still defended itself effectively.[185] The *Tallinn* experts felt that "if the initiator is merely acquiring the capability to initiate an armed attack in the future, the criterion of imminence is not met."[186] Under this reading, developing cyber-strategy, exploits, and even placing botnets in a position to be remotely activated do not meet the imminence standard. However, such distinctions are difficult to make effectively in real-life cyber operations because the speed of attack is almost instantaneous, and the attack can be launched without any of the warning signs, like troop or naval movements visible from satellite reconnaissance.[187]

B. STATE PRACTICE

It is important to note the deference to normal state practice in assessing these issues. The *Tallinn* experts acknowledged that "as cyber threats and opportunities continue to emerge and evolve, State practice may alter contemporary interpretations and applications of the *jus ad bellum* in

179. Glennon, *supra* note 1, at 88–90.

180. *See, e.g.*, Jennifer Trahan, *A Meaningful Definition of the Crime of Aggression: A Response to Michael Glennon*, 33 U. PA. J. INT'L L. 907, 927 (2012) (asserting that the converse "is a nonsensical reading of the text").

181. TALLINN, *supra* note 149, at 63.

182. *See id.*

183. *Id.*

184. *Id.* at 64.

185. *Id.* The notion of imminence in self-defense arises from the U.S. Secretary of State Daniel Webster's correspondence following the nineteenth-century *Caroline* incident, when British forces in Canada attacked a U.S. steamboat for providing aid to Canadian rebels. The "*Caroline* test" is the standard for anticipatory self-defense, applying when the "necessity of self-defense is instant, overwhelming, leaving no choice of means, and no moment for deliberation. *Id.* at 64.

186. *Id.* at 65.

187. *Id.*

the cyber context."[188] In addition to standardization efforts that factor state consensus into their rubric (like the *Tallinn Manual*) direct state practice can also have a major impact on the international understanding of the use of "armed force." Keeping this in mind, it is almost impossible to ignore the state practice and interpretive guidance put forth by the United States, the country with the world's largest military budget and most advanced military technology.[189]

In September 2012, U.S. State Department Legal Advisor Harold Koh addressed the US CYBERCOM Inter-Agency Legal Conference on how to apply the traditional laws of conflict to cyber-operations.[190] Both Koh and the *Tallinn Manual* agreed on the fundamental notion that international *jus ad bellum* principles constraining the use of force apply to cyber-operations and rejected the notion that an entirely new body of law was needed.[191] Both Koh and the *Tallinn* experts also agreed that the *jus in bello* notion of proportionality applied to cyber-weapons.[192] In fact, on many other points there was agreement between *Tallinn* and the official U.S. position as stated by Koh. However, there are two exceptions to this general agreement: one, the threshold at which the use of force enables a state to conduct self-defensive attacks and, two, the meaning of "imminence" in preemptive defensive actions.[193]

After *Nicaragua*, the United States asserted that there is no difference between an unlawful use of force and an armed attack allowing the right of self-defense.[194] Koh reiterated this position in his speech, saying:

> [T]he United States has for a long time taken the position that the inherent right of self-defense potentially applies against any illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response.[195]

188. *Id.* at 42.

189. U.S. expenditures amount to 41% of total world military spending in 2011. Anup Shah, *World Military Spending*, GLOBAL ISSUES, http://www.globalissues.org/article/75/world-military-spending#InContextUSMilitarySpendingVersusRestoftheWorld (last updated May 6, 2012).

190. Harold Hongju Koh, *International Law in Cyberspace*, U.S. DEP'T OF STATE (Sept. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm [hereinafter *Koh on Cyberspace*].

191. Schmitt, *supra* note 116, at 17.

192. *Id.* at 25–26.

193. TALLINN, *supra* note 149, at 47.

194. *Koh on Cyberspace*, *supra* note 190; TALLINN, *supra* note 149, at 47.

195. *Koh on Cyberspace*, *supra* note 190.

In short, the U.S. position is that any unlawful use of force may trigger the right to defensive counterattack. This was not the position of the *Tallinn* experts, nor does it reflect international consensus.[196] This discrepancy between state practice and international consensus may result in situations where a state like the U.S. sees its own action as cyber-defense while other states taking a more mainstream viewpoint might see it as a cyber-attack.

The second point addresses the discrepancies between *Tallinn* and U.S. understandings of "imminence." Under both *Tallinn* and the U.S. position, the Stuxnet attack on Iranian nuclear centrifuges was a "use of force." Standing alone, this use of force may have even risen to the level of an "armed attack" to many of the *Tallinn* experts, which would allow Iran to defend itself under Article 51. The U.S., however, would maintain that its action was in "anticipatory self-defense," legitimate under both *Tallinn* and international law.[197] The resolution to this question turns on the connotation of "imminence." The standard agreed upon by the majority of the *Tallinn* experts, the "last feasible window of opportunity" standard, posits that a state may engage in anticipatory self-defense only when "the attacker is clearly committed to launching an armed attack and the victim State will lose its opportunity to effectively defend itself unless it acts."[198] Clearly this was not the case with respect to Iran's nuclear centrifuges, which were at least two years away from producing enough material for even a single atomic bomb, under most credible measures.[199] According to the U.S. reading of *Nicaragua*, Iran would be justified in taking proportional self-defensive action in response to Stuxnet but for a highly contentious conception of the standard of imminence which permits anticipatory self-defense—a standard which is contradicted by *Tallinn*, *Caroline*,[200] and international understandings of imminence.

Beyond its official statements, U.S. strategic behavior also has a significant impact. By most measures, the United States is rapidly escalating its capacity for cyber defense, cyberattack, and cyber warfare. The terminology that military and political leaders use to describe these

196. TALLINN, *supra* note 149, at 47.

197. *Id.* at 64.

198. *Id.*

199. William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

200. *See supra* note 185.

efforts leaves little doubt as to their effect and purpose: the United States is building its own cyber-military-industrial complex to rival its other military industries. General Martin Dempsey, chairman of the Joint Chiefs of Staff, has asserted that "a cyber-attack could stop our society in its tracks," and has often said that the world is more dangerous now than it was during the Cold War.[201] Defense Secretary Leon Panetta has characterized the threats to the United States as a coming "cyber-Pearl Harbor."[202] Under the leadership of General Dempsey and Secretary Panetta, and that of former President George W. Bush's Director of National Intelligence Michael McConnell, the Defense Department has assembled an array of military contractors to build offensive cyber-weapons. These contractors include the firms Northrup Grumman, Raytheon, General Dynamics, Endgame, and Immunity; in addition, the U.S. may employ the zero-day wares of individual "black-hat" hackers sold from shadow internet chat rooms.[203] The Department of Defense has also invested substantial sums in testing and training facilities in order to "practice" cyber-war, notably the National Cyber Range recently transferred to U.S. Cyber Command.[204] The various U.S. departments spend at least ten billion dollars annually on these efforts, though the exact amounts are classified.[205]

While building this infrastructure, the U.S has repeatedly characterized its efforts as focusing on defensive measures and cyber-security. However, in March 2013, the U.S. government publicly admitted for the first time that it was developing "offensive cyber-weapons." General Keith Alexander, chief of the new U.S. Cyber Command and head

201. Bryan Bender, *World More Dangerous, Top General Says*, BOSTON GLOBE (Apr. 12, 2012), http://www.bostonglobe.com/news/nation/2012/04/12/world-more-dangerous-top-general-tells-harvard-world-more-dangerous-top-general-tells-harvard/XrSM8cTzyZ0YstKv36JhJN/story.html?camp=pm.

202. Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES (Oct. 11, 2012), http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

203. Michael Riley & Ashlee Vance, *Cyber Weapons: The New Arms Race*, BUSINESSWEEK (July 20, 2011), http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html.

204. Sean Gallagher, *"Live-Fire" Cyberwar-in-a-Box Tests Mettle of Military, IT Pros*, ARSTECHNICA (Oct. 20, 2012), http://arstechnica.com/information-technology/2012/10/live-fire-cyberwar-in-a-box-tests-mettle-of-military-it-pros/.

205. Not all defense and intelligence officials agree that the hype is justified. *See, e.g.*, Kim Zetter, *Tone Down the Cyberwarfare Rhetoric, Expert Urges Congress*, WIRED (Mar. 20, 2013), http://www.wired.com/threatlevel/2013/03/tone-down-cyberwar-rhetoric/; Kim Zetter, *Spy Chief Says Little Danger of Cyber 'Pearl Harbor' in Next Two Years*, WIRED (Mar. 12, 2013), http://www.wired.com/threatlevel/2013/03/no-cyber-pearl-harbor/.

of the National Security Agency (NSA), reported in testimony before Congress that "this team, this defend-the-nation team, is not a defensive team. This is an offensive team. . . . Thirteen of the teams that we're creating are for that mission alone."[206] The recent pronouncements, coming in the wake of news of possible Chinese Army-sponsored attacks on U.S. infrastructure,[207] indicate a strategy shift toward a doctrine of preemptive self-defense—an established U.S. doctrine in traditional armaments, but a controversial doctrine under international law and *Tallinn*.

This news follows reports in February that a secret legal review had concluded that the President had the power to order a preemptive cyber-strike if the U.S. foresees a foreign cyberattack based on "credible evidence."[208] These rules were developed under the leadership of John Brennan, recently promoted to the head of the C.I.A. under the Obama administration.[209] This new policy has remained secret, both to protect the President from legal scrutiny and to "maintain ambiguity in an adversary's mind" as to what threshold of action the United States would consider worthy of preemptive attack.[210]

On the legislative front, the U.S. House of Representatives recently passed the Cyber Intelligence Sharing and Protection Act ("CISPA"). This bill has the laudable goal of enhancing cooperation between the government and private companies on cyber-security efforts, but would also transfer supervisory control over national cyber-security efforts from the Department of Homeland Security, where it now resides under Executive Order, to the military.[211] The House version of CISPA also does

206. Mark Mazzetti & David E. Sanger, *Security Leader Says U.S. Would Retaliate Against Cyberattacks*, N.Y. TIMES (Mar. 12, 2013), http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?_r=0.

207. *See supra* Part III.A.

208. David E. Sanger & Thom Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, N.Y. TIMES (Feb. 3, 2013), http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=all&_r=0.

209. *Id.*

210. *Id.*

211. *Executive Order—Improving Critical Infrastructure Cybersecurity*, WHITE HOUSE (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

not limit the power of private companies to "hack back" against attackers of their networks,[212] despite the repeated criticism of security experts.[213]

The collective impact that rhetoric, saber-rattling, funding efforts, and the transfer of cyber-security capabilities to military control can have on lowering the standard for what constitutes cyber-aggression is substantial. To put it another way, each time the U.S. responds to an intrusion with saber-rattling[214] or sounds the drums of cyber-war, it has the effect of *lowering* the "gravity and scale" (or alternatively, "scale and effects") foundation on which a manifest act of aggression rests. The two aspects of U.S. policy seem at odds with one another. On one hand, the military and defense establishment advocate for a basically unrestricted definition of aggression not limited by distinctions between the use of force and armed attack, one which consistently erodes our notion of "attack." On the other hand, U.S. political leaders advocate for a very high threshold for defining an aggressive act of force before the ICC. Cynically, one might conclude that these policy differences reflect the desire of the U.S. to be able to use its cyber-operations machinery to attack or threaten when it suits political ends, but still be able to protect the civilian and military decision-makers who ordered the operations from prosecution by the ICC. At the very least, they expose a dichotomy between the notions of culpability for state-to-state aggression (as proscribed by the U.N. Charter) and individual culpability for that same act (under the ICC). Practically, this places the U.S. between the horns of a dilemma in its public policy: as it tries to make cyber war look imminent for political and budgetary reasons, it becomes more likely that its own cyber-operations might be interpreted as acts of aggression.

This effectively creates discord in international law between the definition of force as understood under the crime-of-aggression analysis and the definition as understood under *jus ad bellum* analysis. This disharmony was reflected in the last-minute Kampala debate over whether the crime of aggression's definitions would be viewed as customary

212. Chris O'Brien, *House Passes CISPA, Sets Up Showdown with White House and Senate*, L.A. TIMES (Apr. 18, 2013), http://www.latimes.com/business/technology/la-fi-tn-house-passes-cispa-20130417,0,7501025.story.

213. *See generally* Bruce Schneier, *Schneier on Security*, http://www.schneier.com/.

214. *See, e.g.*, Mazzetti & Sanger, *supra* note 206.

international law. To determine whether these two definitions are equivalent, observers will have to wait for the ICC to bring its first cases.

VII. INDIVIDUAL COMMAND AUTHORITY OVER STATE ACTS

While the threshold clause and other modifiers limit the crime of aggression's applicability to cyber-aggression, the crime has other elements that effectively narrow its reach even further. The crime must be committed "by a person in a position effectively to exercise control over or to direct the political or military action of a State."[215] This restriction is sometimes known as the "leadership clause," and it is reemphasized again in Element 2 of the crime. Element 2 also clarifies, in case Article 8 *bis*, paragraph 2 left it ambiguous, that the act of aggression must be "committed" by the state, not merely planned, prepared, or threatened. On the other hand, an individual may be culpable for his contribution to a fully realized act of aggression under any of the typical Rome Charter "conduct verbs," including planning, preparing, initiating, or executing the act.[216]

At the outset, it is clear that the leadership clause severely restricts whether the crime applies to the sort of cyber-operations routinely conducted today. Consider, for example, the Georgian DDoS attacks. If the DDoS attacks were perpetrated by non-governmental groups in Russia who merely sympathized with the Russian government's position—and even if they coincided with conventional Russian aggressive action—the hackers who coordinated the attacks cannot be held accountable under the leadership clause because they failed to possess any control over military or political forces. On the other hand, some cyberattacks clearly do meet the requirements of the leadership clause. Whether or not formally acknowledged by officials, substantial evidence suggests that Stuxnet was conceived, planned, and executed at the highest levels of the U.S. government, up to and including Presidents Obama and George W. Bush.[217] An even more verifiably culpable actor is the head of Mossad, Israel's national intelligence agency, who trumpeted the success of the Stuxnet program to journalists in 2011.[218]

215. Rome Statute, *supra* note 6, art. 8 *bis*, para. 1.
216. Kampala Compromise, *supra* note 12, ann. II, Elements, para. 1.
217. *See supra* Part III.A.
218. Stark, *supra* note 26.

This debate turns on the definition of "effectively to exercise control over." There is some evidence that even this language reflects a softening of positions during the negotiations: some early formulations mentioned only "direct control."[219] On the opposite extreme, another formulation considered whether persons who "shape or influence" the state's action might also be included; however, it was believed that this language would be problematic for democracies, wherein a large number of people might be in a position to shape or influence policy.[220] Under the resolved formulation, if, as one Russian minister claimed during an interview about the cyberattacks against Estonia, "that attack was carried out by my assistant,"[221] then his aide was possibly culpable for planning and initiating. The question hinges[222] on whether the aide had "effective control" over the political or military action of the state, but that term certainly leaves interpretive space for *de facto* authority as well as *de jure* authority.

The aforementioned example is relatively straightforward; nevertheless, the question can be much more subtle because cyber-operations are often conducted in organizational structures of loose control. Hackers typically lack authority or control over any other person. Clearly, many cyber-operations lack the rigid command hierarchy of the military chain-of-command or executive-branch bureaucracy, and yet loose groups, such as the hacker collective Anonymous, can still coordinate and conduct operations with relative effectiveness. Moreover, such loose organizations reflect not an exception in warfare but rather an underlying trend that military planners have observed for at least two decades.[223] In fact, some experts have gone so far as to "forecast the future irrelevance of state-on-

219. Barriga, *supra* note 3, at 21.

220. *Id*. at 22.

221. *Behind the Estonia Cyberattacks*, RADIO FREE EUR. (Mar. 6, 2009), http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html.

222. This assumes, of course, that DDoS attacks are an act of aggression meeting the threshold clause.

223. *See* Weisbord, *Conceptualizing Aggression*, *supra* note 83, at 14–16 ("Despite their different perspectives on the future of the state, these forecasters point in a similar direction—most fundamentally, towards the decentralization of armed conflict—that few experts today dispute. If accurate, the literature on the transformation of war has important repercussions on the way aggression should be conceptualized and regulated.").

state warfare."[224] Under the current formulation, if strictly interpreted, individuals in terrorist groups like al Qaeda could not be tried for the crime of aggression because they lack effective control over a "state" in the formal sense—even though the leaders of al Qaeda clearly have effective political and military control over some entity. To address these concerns, Weisbord has proposed a broader conception of "state" than is in common usage, one that leaves room for jurists to consider effective control over "state-like" entities such as al Qaeda.[225] On the other hand, even Weisbord's proposed reading of "state" would not encompass loose collectives of nationalist hackers.[226]

The doctrine of Joint Criminal Enterprise ("JCE"), first enunciated by the ICTY and later codified in Article 25(3)(d) of the Rome Statute, is an interpretive tool that may be able to mitigate some of the difficulties of applying the crime to the loose organizational models behind cyberattacks.[227] JCE is broadly applicable to all crimes prohibited by the Rome Statute and recognizes that many of the atrocities condemned by the Rome Statute rely on the participation of groups that are not under the direct control of the government.[228] JCE also recognizes that it may not always be clear what "political or military leadership" is, especially in situations where multiple factions are all claiming legitimacy. JCE may well allow the prosecution of additional groups who contributed to the "common purpose" of committing the act of aggression, and therefore permit the ICC to expand culpability beyond the leaders of the directly responsible group to those in supporting groups.[229] The ICC may also interpret JCE to permit the leaders of non-state organizations that aid in the common purpose to be held accountable, such as the head of a nationalist group who directs its hackers to conduct a cyberattack. The question will turn on whether the ICC imputes the leadership clause restriction only to the directly responsible group or also to the groups who assist in the common purpose.

224. *Id.* at 14 (interpreting the assessments of military historian Martin van Creveld and counterterrorism expert John Robb).

225. *Id.* at 30. *Accord* Kai Ambos, *The Crime of Aggression After Kampala*, 53 GERMAN Y.B. OF INT'L L. 463, *23 (2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1972173.

226. *See* Ambos, *supra* note 225.

227. Rome Statute, *supra* note 6, art. 25, para. 3(d).

228. The Rwanda atrocities, for example.

229. Weisbord, *Judging Aggression*, *supra* note 1, at 92.

A consequence of the leadership clause is that it exacerbates the attribution problem that is common to all cyberattacks; the difficulty of attribution would seem much less significant if the responsible parties, whoever they were, could be brought to justice. This consequence brings to light a latent normative question: why should individuals who are trying to start a war between two states by perpetrating an act of aggression—irrespective of whether they control the state's military or political apparatus—*not* be subject to criminal prosecution? It has been difficult for commentators, and the parties themselves, to vocalize a precise answer to this question. The difficulty probably stems from the original use of Resolution 3314 and its emphasis on the "state-oriented" perspective. From that viewpoint, it perhaps seems expansive and slightly uncomfortable for states to begin extending culpability in this way. However, this is not a compelling rationale because individual members of non-state entities are clearly within reach of the Prosecutor for other ICC crimes, such as crimes against humanity.[230] As Kai Ambos states:

> [T]he human being oriented approach of international criminal law, focusing on individual criminal responsibility, strongly suggests the inclusion of non-state actors. The essence of the crime of aggression is not so much determined by the actor but by the wrongfulness of the act. . . . [T]he drafters [should have inquired] more fundamentally [into] the interests and values to be protected by a modern crime of aggression.[231]

VIII. CONCLUSION: PROSPECTS, ALTERNATIVES, AND THE FUTURE

Is there any hope that the crime of aggression will be successful in curbing cyber-aggression? The analysis above suggests that the definitions and elements of the crime can be interpreted broadly enough to encompass the newer forms of aggression, including cyberattacks. On one level, it is quite clear from the negotiation history that the flexibility to adapt over time was the intention of the parties and was the bargain behind their compromises. Beyond that, however, adaptation of international norms to new forms of aggression—manifested through different attack methods and implemented with new organizational structures—*must* occur because the

230. STEVEN R. RATNER ET AL., ACCOUNTABILITY FOR HUMAN RIGHTS ATROCITIES IN INTERNATIONAL LAW 70 (3d ed., 2009).

231. Ambos, *supra* note 225, at *19–20.

form and function of aggressive conduct is inexorably changing. State practice and understanding will morph international expectations and customary international law.

On a more normative level, the sixty-five-year endeavor to define aggression indicates something important about the human instinct: as human beings and societies, we want to promote peace by making aggression a punishable offense. The crime's inclusion in the Rome Charter, alongside but in context with other heinous crimes like genocide and war crimes, tells us that, when the time comes to decide whether an aggressive act meets the threshold clause, jurists have some flexibility. Dire civilian effects, for example, may be good evidence of gravity and scale, but not necessary for manifest breaches because they would be covered by other ICC crimes. The real crime of aggression is the threat to peace, and jurists may evaluate the act of aggression in such a way that conceptual space exists between the various ICC crimes. This is within the judges' mandate under the preamble to end "impunity for atrocity crimes."[232] Taking their cue from the Travaux Préparatoires, the judges should interpret the crime in a way that "promotes peace."[233] Indeed, according to one commentator, "the task of ICC judges is to interpret the new prohibition on aggression within the language of the ICC Statute to advance its retributivist and expressivist goals *in such a way as to promote peace and security*."[234]

However, restraints on jurisdiction and political concerns *vis á vis* the U.N. Security Council will ensure that the individual crime of aggression is the last thing punished, even after state sanctions or counterattacks are levied under U.N. Charter authority. For that reason, developments in the *jus ad bellum* such as the *Tallinn Manual* may have more of an impact on curbing cyber-aggression than the ICC crime of aggression. Ultimately, a widening chasm may form between what is required for individual accountability versus what is required for state accountability for aggression. If those standards do not coincide, the world will continue to have largely politicized state culpability for acts of aggression but very little individual accountability. Even so, for some commentators, this is a natural—and perhaps desired—consequence:

232. Weisbord, *Judging Aggression*, *supra* note 1, at 121.
233. *Id.* at 120.
234. *Id.* at 122 (emphasis added).

> It is true, though, that the requirements of a "manifest violation of the Charter of the United Nations" will make successful proceedings for a crime of aggression an exceptional event. But what is wrong with this consequence? Is international criminal law (*stricto sensu*) not an instrument for exceptionally grave assaults upon the international legal order to be applied with utmost restraint? An expansionist resort to international criminal law must lead to its trivialization. This is true for crimes of aggression as it is for all other crimes under international law.[235]

If indeed there is little confidence that the newly defined crime of aggression will curb offensive cyber-operations before they escalate to chilling heights, less politically hazardous approaches to the problem are worth pursuing. Diplomacy, moral example, de-escalation of rhetoric, treaties, and a policy emphasis on defensive technical approaches all have a place in helping to quell aggression before it rises to the level of war.

Diplomacy, moral example, and de-amplification of rhetoric can have stabilizing effects on aggression for the same reasons that escalating rhetoric brings more behaviors under the umbrella of aggression. Recently, for example, President Obama attempted to quell the firestorm of words resulting from publication of the Mandiant Report by asking the Chinese government to recognize the threat these activities posed to its international credibility and to "engage in constructive direct dialogue to establish acceptable norms of behavior in cyberspace."[236] The President implied that cooperation was necessary between the U.S. and China because, regardless of whether the cyberattacks were sanctioned by the Chinese government, they originated from Chinese soil.[237] In response, China called for new international standards and the countries held military talks in April 2013.[238] A senior Chinese general pledged to work with the U.S. on cyber security "because the consequences of a major cyberattack 'may be as

235. Claus Kress, *Time for Decision: Some Thoughts on the Immediate Future of the Crime of Aggression: A Reply to Andreas Paulus*, 20 EUR. J. INT'L L. 1129, 1142 (2009).

236. Sean Gallagher, *White House Asks China to Stop Hacking, Pretty Please*, ARSTECHNICA (Mar. 12, 2013), http://arstechnica.com/tech-policy/2013/03/white-house-asks-china-to-stop-hacking-pretty-please/.

237. *Id.*

238. Jane Perlez, *U.S. and China Put Focus on Cybersecurity*, N.Y. TIMES (Apr. 22, 2013), http://www.nytimes.com/2013/04/23/world/asia/united-states-and-china-hold-military-talks-with-cybersecurity-a-focus.html?ref=todayspaper&_r=0.

serious as a nuclear bomb.'"[239] It is unknown what fruit these efforts will bear, but the President's softening of tone has allowed the Chinese to "save face" while coming together to talk.

Cooperative efforts that create international standards can also impact the debate in positive ways. In 2011, the International Telecommunication Union ("ITU") published a report advocating for "cyber peace."[240] The report argued that, while loose conceptions of "cyber-war" were plentiful, these conceptions framed the problem in the negative.[241] Instead, a positive definition of a peaceful, non-aggressive cyberspace was needed.[242] Proceeding from this ethical framework, the report details concrete principles and suggestions for cooperation between nations and prioritizes defensive activities over offensive strategies.[243]

Defense should be distinguished from *deterrence*, in which a state "defends" itself by having the largest arsenal of offensive weapons. So far, military planning concepts from the Cold War have also ruled the "cyber-war" epoch. Reducing cyber-aggression requires abandoning the traditional "offense dominates defense" mentality which has controlled the cyber war tactical debate to this point. When countries focus on building offensive cyber-arsenals, they not only advance the craft of malware development, which, over time, escalates aggressors' capabilities to more dangerous levels; they also encourage marketplaces for the mercenary development of malware, establishing an arms trade in cyber-weapons.

Instead of offense, governments and technicians from both public and private sectors should focus their efforts on developing secure, transparent standards for the technologies that run computer networks, as well as on sharing information about threats to technological infrastructure. Sadly, recent attempts by the ITU[244] to pass implementing proposals to require its member-states to meet certain obligations with respect to internet security were branded by the U.S. Delegation as "a U.N. takeover of the

239. *Id.*

240. DR. HAMADOUN I. TOURÉ, ET AL., THE QUEST FOR CYBER PEACE (2011), *available at* http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf.

241. *Id.* at 77.

242. *Id.* at 78.

243. *Id.* at 84. Contrast this to CISPA, for example, and its emphasis on active defense and counterattack. *See* O'Brien, *supra* note 212.

244. These attempts occurred at the World Conference on International Telecommunications, held in Dubai in December 2012.

Internet."[245] The U.S. successfully derailed the proposals, ensuring that *de facto* U.S. control of Internet standards bodies continued.[246]

These are a few of the concerted efforts that will be needed to quell cyber-aggression, and each is difficult to accomplish in its own right. Whether the Kampala Compromise will play any part in achieving a peaceful cyberspace remains to be seen, but if judges take their mandate to promote peace and security seriously, the ICC "can help avoid some conflicts, prevent some victimization, and bring to justice some of the perpetrators of these crimes. In doing so, the ICC will strengthen world order and contribute to world peace and security. . . [and] will add its contribution to the humanization of our civilization."[247]

245. Eli Dourado, *Behind Closed Doors at the UN's Attempted "Takeover of the Internet"*, ARSTECHNICA (Dec. 20, 2012), http://arstechnica.com/tech-policy/2012/12/behind-closed-doors-at-the-uns-attempted-takeover-of-the-internet/.

246. *Id.*

247. BASSIOUNI, *supra* note 2, at 649 (author's speech delivered at the Rome Ceremony on July 18, 1998, after the signing of the Rome Charter).