



Conference Brief

INTERNATIONAL LAW DEPARTMENT
Center for Naval Warfare Studies
United States Naval War College

Sponsored by

*The United States Naval War College and
United States Cyber Command*

with generous support from

*The Naval War College Foundation
The Swedish National Defense College
The Israel Yearbook on Human Rights*

*The International Institute of Humanitarian Law, Sanremo Italy, and
The Lieber Society on the Law of Armed Conflict, American Society of International Law*

Cyber War and International Law

Compiled by

Commander Christian P. Fleming, JAGC, U.S. Navy

From June 25 - 27, 2012, the United States Naval War College brought together operators, policy makers, technical experts, and legal scholars to participate in a conference examining the legal norms that govern both cyber strategies and the use of cyber capabilities during armed conflict and other military operations. The conference featured three keynote addresses and nine panel discussions.

Key Insights:

1. Cyber is a new weapon, but the *lex lata* of the law of armed conflict (LOAC) is sufficient to regulate cyber warfare and applies to cyber just as it would apply to any other weapon.
2. To determine whether an operation using only cyber constitutes an attack in the *jus in bello* sense, the consequences of the operation need to be examined. A cyber operation causing death, injury, or destruction is an attack, as would interference with the functionality of an object resulting in damage. Damage includes the requirement of reloading an operating system. Mere denial of service is not an attack.
3. A response to a cyber attack can be kinetic, just like a response to a kinetic attack can be by cyber.
4. Cyber weapons such as malware, viruses, and worms have the potential to be indiscriminate. Operational lawyers should conduct weapons reviews of cyber weapons just as they would for kinetic weapons, as well as giving targeting advice for specific operations.



PANEL I:

An Introduction to Cyber Operations

Panel I, moderated by Lieutenant Commander Paul Walker, JAGC, USN, of U.S. Cyber Command, consisted of Colonel Ronald Reed, USAF (Ret.), of Microsoft Corporation; Captain Timothy J. White, USN, of the Navy Information Operation Command Maryland; and Mr. Eric Greenwald of U.S. Cyber Command.

Colonel Reed spoke to the cyber strategy of the United States. Joint Task Force on Computer Network Defense (JTF-CND), a precursor to U.S. Cyber Command, was stood up in 1998. New organizations generally stand up after disasters. But in 1998, there was recognition that there were threats that had to be addressed because the network defenses in place at the time were not sufficient. In response, the command became Joint Task Force - Global Network Operations (JTF-GNO). In 2003-2005, there were a number of incursions of a significant nature into Department of Defense networks, and it became apparent that the way the Department of Defense was organized was not sufficient to deal with the developing threat from cyber, leading to the creation of Joint Functional Component Command - Network Warfare (JFCC-NW). However, there were gaps, and so JFCC-NW and JTF-GNO merged into U.S. Cyber Command. Turning to the perspective from industry, Colonel Reed stated there is a recognition that cyber is a domain with shared characteristics, akin to the commons. The need for access to cyber and transit through it are critically

important. Industries are concerned with profiting from cyber, so the amount of money spent on securing cyber from threats is increasing. We are moving into a “cloud” environment. The issue for the military is that when operations occur in the cloud, a single network is not targeted, but an entire domain with both military and civilian interests. Industry is taking matters into its own hands to take offensive operations. One of the issues with operations, though, is attribution of who has launched a cyber attack. The legal regime, from a business perspective, desires laws that enhance the cyber domain for consumers.

Captain White discussed the building of U.S. Cyber Command. He explained there were external actors and internal structural deficiencies driving the process of standing up Cyber Command. In 2008, while engaged in active operations in Afghanistan, the potential compromise of data security and integrity of data led to a loss of confidence in command and control. That was a driving factor in examining what steps were necessary to secure cyber. There was a mobilization around this imperative with a clarification of terms and consultation with lawyers. JFCC-NW and JTF-GNO came together in the fall of 2009 to form Cyber Command, organized as a subordinate unified command under U.S. Strategic Command. The mission of Cyber Command is how to contribute to defending the nation, and how to support the mission around and across the globe. In cyber, we need to be able to see, understand, and prepare for various threats. State and non-state actors are getting better at exploitation. From the U.S. standpoint, we were static. We are



now growing ever more interconnected. As a consequence, there is high vulnerability. The purpose of Cyber Command is to take experts at conducting operations and experts at network defense, and mobilize them under one command.

Mr. Greenwald addressed the intersection of intelligence and military operations. His basic idea was that cyber operations that fall below the level of use of force should be regulated under international law in the same way as espionage, which is to say that they are not expressly permitted nor expressly prohibited. First, he discussed how cyber operations are treated under U.S. domestic law and international law. The law of military operations, intelligence operations, and covert operations overlap but there are distinctions. It is not always perfectly clear where cyber operations fall, because even when cyber operations are conducted as a military action, they still have similarities to intelligence and covert actions. Traditionally, the three types of actions were supposed to be distinct from each other, but cyber operations are difficult to categorize. Under international law, cyber operations can be put in one of two categories: ones that rise above the use of force, and ones that fall below. In analyzing whether the operation falls above or below the use of force threshold, cyber shares the same issues that exist in the kinetic realm. There are not precise lines in either domain. While there may be more of a grey area in cyber, this is due in part because there is less experience here. For cyber operations that rise above the use of force, the same legal regime of *jus ad bellum* and *jus in bello* apply as in kinetic operations. There is difficulty in

regulating cyber operations that fall below the use of force in any manner other than in a manner consistent with how espionage is treated. Mr. Greenwald does not see much hope in new accords to regulate these types of cyber activities. No one wants cyber activities to occur on their soil, but states are not willing to forego the opportunity to conduct cyber activities against others. So, cyber activities below the threshold will enter the same realm as espionage, that is to say, international law effectively being silent.

KEYNOTE ADDRESS:

Professor Jack L. Goldsmith
Henry L. Shattuck Professor of Law,
Harvard University

The thesis of Professor Goldsmith's presentation "Law and Cybersecurity: A Pessimistic Assessment" is that the digital revolution creates large structural gaps in effective legal regulation that significantly disadvantage U.S. national security, broadly conceived, that are very hard to close through traditional legal means.

Professor Goldsmith began by describing the pre-cyber legal framework for regulating threats from abroad. Before cyber existed, geography was a barrier to attacks from abroad. Domestic law, to the extent that a person or his assets were located in the United States, and international criminal law, to the extent the person could be extradited, were means of regulation. *Jus ad bellum* put limits on the use of force by other states against our country. Deterrence through reaction was also employed to limit threats from abroad. Espionage was never regulated by international law, but only by domestic



criminal law. This system led to gaps in our national security but, on balance, did a good job of checking threats from abroad prior to the digital age.

After addressing the characteristics of the cyber problem, such as the growing interdependence of states, the fact that distance can be obliterated, the difficulty of attribution, the muddling of the public/private distinction, the muddling of the domestic/international distinction, the empowerment of adversaries, and the secret cyber arms race, Professor Goldsmith commented that the legal response has been to apply the pre-cyber legal tools by analogy with little change in the law. He notes that the problem with this response is that cyber creates a huge gap between the threat and the legal effectiveness available to address the threat. The threat is growing much faster than the legal, political, and military responses, and the gaps are difficult to close by law.

Turning to cyber espionage, Professor Goldsmith noted that exploitation is widespread. Cyber espionage could be a precursor to an attack. The law is useless against all but local insider threats because espionage is unregulated by international law, poorly regulated by domestic law, and not redressable by military means.

As for cyber attack, attribution and deterrence are difficult. And, there are legal gaps because the analogy to kinetic attacks downplays damaging cyber attacks, such as attacks against economic targets. A kinetic response to all but the most extreme and public of attacks would

be difficult to justify. Poor deterrence emboldens adversaries.

The United States is asymmetrically vulnerable because it is more dependent than most states on computer networks and communications technology, because it is more restrained than most, and because it has the farthest to fall. The hurdle to raising domestic defenses is a fear of the National Security Agency by the private sector, and because of the financial considerations of paying for adequate security. Unfortunately, there will be no action taken to increase our defenses until there is a major public cyber event.

KEYNOTE ADDRESS:

Rear Admiral Margaret DeLuca "Peg" Klein, USN
Chief of Staff, U.S. Cyber Command

Read Admiral Klein addressed the aspects of cyber space. Cyber space is a defining feature of modern life. The United States relies on cyber space for its international and national security. Modern forces require reliable access to cyber space, and operators face challenges in conducting cyber operations. The legal community should determine how new laws and policies apply. The lack of clear legal guidance is comparable to other periods of technological advance, such as the early 19th Century with the advent of the telegraph, and then the 20th Century with the advent of the airplane. Cyber is a new technology that merges national security components, such as espionage and war fighting. Military non-intelligence operations conducted in cyber space



should follow the same rules as those conducted in the kinetic world. Death, injury, and damage are uses of force, but what level of damage in cyber space would qualify? And what level of force would rise to an armed attack? Often cyber operations are not destructive, so how is the correct response determined? If operations fall below the use of force, then proportionate countermeasures are permitted. But how much attribution is needed? Can we hold a state responsible for failing to prevent cyber operations from its own territory? The identity of the combatant is also muddled due to the ease of entry onto the battlefield. Applying the rule of distinction becomes difficult because of dual use issues. There are significant practical challenges of conducting operations in cyber space, and doctrine needs to be developed. A cyber operations field manual is necessary, and it must be shown that the tactics, techniques, and procedures that are developed for cyber space function.

PANEL II: Organizing for Cyber Operations

Lieutenant Colonel Lisa Gumbs, JA, USA, moderated this panel, consisting of Mr. Stewart A. Baker of Steptoe & Johnson and Mr. Mark D. Young of U.S. Cyber Command.

Mr. Baker discussed the role of the United States government and the intelligence community in cyber operations. Why cyber war, he posited? He answered because it is a two-for-one deal. Cyber operations can be a run-up to war, wherein

the enemy's own network is used to spy against him, and then on the first day of the war, his system can be killed, denying him use of what was just used against him. Supervisory Control and Data Acquisition (SCADA) systems are in the bulls-eye because they are critical and easy to attack. Making sure our own system stays up is critical. The response to cyber threats is to attack, defend, negotiate, or lawyer-up. The problem with attacking is the issue of attribution, but this issue can be addressed through technology. The way to defend is to go after the attackers and make them hurt more than they hurt us.

Mr. Young described legal support for Department of Defense cyber operations. He began with background on how planning is conducted for U.S. military forces, and said that military action should be an option in cyber space. Then he asked what it means to mobilize cyber forces, and what sustainment of cyber forces means. Most of what is performed in Cyber Command are not offensive operations but defense of the Department of Defense (DoD) network, with a support role for protecting non-DoD information systems. Mr. Young described the process of targeting in cyber, saying it was effects based to achieve certain objectives and interdisciplinary. Turning to cyber security, the DoD has robust domestic authority to conduct internal network operations. He then reviewed domestic legal authorities for the DoD to take various defensive and offensive actions to defend its own systems and non-DoD systems. We need to be creative in using the authorizations that we currently have,



and legal creativity fundamentally alters key substantive areas of law.

PANEL III:

**Cyber Attacks:
The Operator's Perspective**

The final panel of the day was moderated by Naval War College Professor Derek S. Reveron. This panel, which discussed cyber attacks from an operator's perspective, consisted of Dr. Deborah Schneider of the U.S. Department of State, Mr. Donald Boian of the National Security Agency, and Major Chris Walls, USA, of U.S. Cyber Command.

Dr. Schneider analyzed foreign policy and cyber operations, specifically addressing sovereignty. The United States respects the sovereignty of other states, and this applies to cyber. There are different aspects to sovereignty, on which states place varying emphasis depending on their national interests. Dr. Schneider described four political science aspects of sovereignty as domestic, interdependence, international legal, and Westphalian, and proposed cyber aspects of each. She opined that through the Convention on Cybercrime (the Budapest Convention), states compromised some on sovereignty. But, further conventions are elusive because some states see the free flow of ideas as the real threat, whereas other states see cyber attacks as the threat. Reciprocity brings restraint, since reciprocity requires a state to act overseas how it would allow other states to act on its soil. Taking unilateral cyber action can make state cooperation on other issues more difficult.

Mr. Boian described cyber threats and vulnerabilities. Intrusions into U.S. systems are happening daily, including intrusions into military, industrial, and financial networks. There are known intrusions, and there are unknown intrusions. Some accounts of the loss of intellectual property assert the amount is one trillion dollars annually. A clear definition of cyber attack is elusive. Defending ourselves requires a team effort across government and private industry. Cyber as a domain is very different from other domains because of the speed of action, the difficulty of governance, the unclear boundaries and geography, the complexity and evolving nature, and the fact that cyber is unchartered. Using traditional military doctrine does not always fit. The acquisition of weapons systems is difficult because the technology changes rapidly. Cyber is asymmetric in that small players can level the playing field. Attribution is difficult because of the use of proxies, and after-the-fact attribution is not enough because we need to know who the attacker is in real time. The adversaries get to pick the time and place of attack. Often, the weakest point to attack is the human factor.

Major Walls was asked to address military cyber operations. He stated that maneuver warfare is relevant in cyber. Old molds can be used to build new ones. We can achieve through cyber what we used to accomplish with a kinetic strike. Expeditionary forces are aided by turning things on or off through cyber. Counterinsurgency cyber operations impact what people think, and the center of gravity in counterinsurgency is what



people believe. Counterterrorism is performed in cyber by finding people and making them predictable in order to plan a potential kinetic strike. And, there are hybrid operations that fall outside of these three models in which conditions are set for future operations against state actors with long-term simmering fights.

PANEL IV:

General Principles of International Law

Day two began with Panel IV. This panel, moderated by Captain Kevin M. Kelly, JAGC, USN, of the U.S. Naval War College, was comprised of Professor Dr. Wolff Heintschel von Heinegg of Europa-Universität Viadrina, Sir Daniel Bethlehem KCMG QC of Legal Policy International Ltd. (LPI), and Professor Robert M. Chesney of the University of Texas School of Law.

Professor Dr. Heintschel von Heinegg focused on sovereignty and neutrality. He began by stating that the concept of sovereignty has been long settled, and quoted the *Island of Palmas* arbitration's definition: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State." In addition to protection, sovereignty imposes obligations of integrity and inviolability in peace and in war. The characteristics of cyber space are ubiquity, anonymity, and interdependent networks. Cyberspace, however, requires a physical architecture to exist, and what is behind it is real.

States can exercise sovereignty and criminal jurisdiction over this architecture. The first consequence of this is that the cyber infrastructure covered by territorial sovereignty is protected against interference by other states. The prohibition of interference is not limited to the unjustified use of force, armed attack, and intervention. The protection of sovereignty goes far beyond these three coercive elements but also to situations below the use of force that would be a violation of the state's sovereignty. The second consequence of the principle of territorial sovereignty applied to cyber space is that there is a wide-ranging right of the territorial state to exercise jurisdiction over the cyber infrastructure located in and the cyber activities occurring in its territory. Further, the effects doctrine entitles a state to exercise jurisdiction over conduct not initiated in its territory but having effects in its territory. There is an obligation of states to terminate violations of territorial sovereignty of another state by actions occurring within its borders. This duty presupposes knowledge of the violation, but not necessarily actual knowledge; presumptive or constructive knowledge could suffice. But, the mere occurrence of a violation is not enough; there must be knowledge. There is no duty of prevention to monitor all activity within a state. The International Strategy for Cyberspace by the President of the United States enumerates five criteria when applying the existing rules to cyber: reliable access, multi-stakeholder governance, global interoperability, network stability, and cyber security due diligence. The U.S. strategy cannot be achieved on a unilateral basis. Like-



minded states are needed to endeavor in a concerted effort to take this path. But, the mere fact that the United States does not like the existing law cannot be a reason to ignore it. Otherwise, the United States would either violate the law or be a lone wolf in the desert. Turning to neutrality, Professor Dr. Heintschel von Heinegg cited it as one of the most contested areas of international law. It presupposes an international armed conflict. The scope of the applicability of the rules on neutrality is far from settled. But, despite the alleged revolutionary character of new technologies, long-standing treaties still apply. The primary objectives of the law of neutrality are to protect the sovereignty of neutral states and to stop the escalation of an ongoing armed conflict. There is wide-spread agreement that the law of neutrality applies to cyber. Belligerents are under an obligation to protect the inviolability of neutral states and to not take hostile acts in the territory of neutral states. It is not yet settled if this obligation pertains to malicious cyber activities transferred through neutral territory. Neutral states are obligated to take all feasible measures to terminate hostile acts on their territory. There is only a duty of prevention where there is actual knowledge that malicious software is being prepared in its territory that will be used against a belligerent. If a state is unwilling or unable to comply with its obligation to terminate a violation of its neutral status, the aggrieved belligerent is entitled to enforce the law of neutrality, subject to proportionality.

Sir Daniel Bethlehem spoke to the legal framework for analyzing cyber operations, and began by commenting that we need to

go beyond the *lex lata* and recognize there are important areas of uncertainty in the legal framework of cyber. Preliminarily, we ought to engage in a deeper inquiry of our competitive and comparative advantage positions. We probably still have a competitive advantage in cyber due to the creativity of our institutions and private companies, but it is unclear if we still have a comparative advantage given the sheer volume of hostile cyber activity. His first proposition is that this is the time to act to craft a more benign legal framework. Second, the debate around cyber is driven too much by U.S. domestic regulations and too much around the U.S. view. The U.S. view is dominated by Title 10/Title50/Title 6 and the First Amendment, whereas the U.K. view is to give a broad authorization for cyber operations. While size matters, so does nimbleness and flexibility. Sir Daniel read the authorization for cyber operations of the U.K. Government Communications Headquarters (GCHQ), and opined there is no comparison to the U.S. authorization. There is no clear divide between war and peace, internal and external, military and police operations. The debate needs to be more informed by reference to international partners. Third, we need to be cautious as to sources of law in cyber because there are very few that are applicable. Fourth, there also needs to be a real appreciation of the end of geography in the sense that the world is flat. International law is too rooted to Westphalian notions of sovereignty, but the world has moved on. Concluding his preliminary remarks, Sir Daniel said we can do better to draft a more benign legal environment. Moving to his main remarks, he stated we should be slow to



default to a *jus in bello* analysis. Not all kinetic operations engage a *jus in bello* analysis, whether it is hostage rescue, U.N. operations against pirates, or military operations in support of police enforcement, for example. Caution is required because a *jus in bello* analysis may not be appropriate to the circumstances. It also could too quickly invite a kinetic response. And, such an analysis could be too permissive, such as with targeting, or too constraining, such as with countermeasures. Additionally, it presumes that espionage is regulated more fully than it is. Finally, such an analysis would expand and confuse the threshold for physical action. A *jus in bello* analysis could be used in some circumstances, but should not be the presumptive default. To determine whether *jus in bello* is appropriate, the following elements should be examined: is the cyber action equivalent to a kinetic operation; is there only non-kinetic injury; is it in support of conventional military operations; is it intended to degrade the target state's capabilities; and, would it cause large-scale economic damage? Also ask would it pass a *jus ad bellum* gateway? Finally, ask whether it is attributable to a state? Sir Daniel concluded that the comparison with the advent of other technologies is not readily analogous, because the international legal framework is well-established now. There is quite a lot of specific treaty law and broad customary law, and the question is how these laws apply to cyberspace. Finally, the law in reference to state responsibility is largely codified and regarded by most as customary international law. Turning to shared operations, the law with regard to attribution becomes complex. There is a

question as to how to organize the legal framework with shared operations because we come from different legal frameworks. Finally, with respect to aiding or assisting, given that we come from different legal frameworks yet we are cooperating, what can we properly do together without engaging questions of legal responsibility?

Professor Chesney discussed Title 10/Title 50 and international law in cyber warfare. The first issue concerns information sharing, meaning reporting requirements to Congress. Specifically, is there such a requirement, and, if so, is the reporting to the intelligence committee or armed services committee? The answer depends on how the cyber operation is characterized. If an operation is characterized as covert action, then there is an obligation under Title 50 to report it. But, the distinction between covert action and traditional military activities is disputed. There is also an exemption to reporting covert actions for activities the primary purpose of which is to collect intelligence rather than to influence events. But, the lines are often blurred and an operation might seem to be one thing when analyzed standing alone, but could be one part of a larger operation that is harder to characterize. The second issue is whether there is an affirmative authorization of any department to carry out cyber operations. It is a separation of powers issue as to whether the executive branch has authority to carry out the operation or whether authorization from Congress is required. Here, the nature of the cyber operation needs to be analyzed to determine whether it lies within the inherent constitutional power of the executive branch. The third issue is



whether the categorization of a cyber operation under U.S. domestic law has an impact on the obligation to comply with international law. The question posed by Professor Chesney is whether our domestic statutory framework gives the executive branch permission to authorize operations that violate international law when operating under Title 50 covert action authority but not under Title 10.

PANEL V: Self-Defense

Panel V focused on self-defense. The panel was moderated by Captain Peter W. Bowers, RAN, Director of Operations and International Law and Director of Navy Legal Services for the Royal Australian Navy, and consisted of Ms. Alexandra Perina of the U.S. Department of State, Professor Matthew C. Waxman of Columbia University, and Professor Terry D. Gill of the Amsterdam Center for International Law, University of Amsterdam.

Ms. Perina discussed use of force under Article 2(4) of the U.N. Charter. There is broad agreement that international law applies to cyber conduct, but some believe that there should be a new international agreement to govern it. One concern may be that the use of force threshold is too low. A clear definition of what constitutes use of force in cyber is elusive, just as it can be in the kinetic realm. A use of force is physical violence, and traditionally excludes economic or political coercion. There is general agreement on how the rules apply in cyber at the far ends of the spectrum. Opening the slush gates on

dams to kill people and knocking out the air traffic control equipment to cause crashes would be clear uses of force. On the other end of the spectrum, hacking and espionage are not uses of force. Conduct falling between the extremes present the difficult cases. There are four tests that have been suggested. First, we could say “we know it when we see it,” but this is unsatisfactory. Second, we could use an instrumentality test and focus on the tools employed. But this is too crude of a test and is widely rejected. Third, an effects test could examine the consequences of the action and whether the damage is akin to that created by a military weapon. Such an analysis could be overinclusive. Finally, a test based on Professor Schmitt’s 1999 “Wired Warfare” article would evaluate the following factors: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy. She also added the context of the attack and the intent of the attacker to the factors to consider. The widespread view is that there is a gap between prohibited uses of force and armed attacks triggering the right of self-defense. The ICJ found that the test of whether a use of force constitutes an armed attack depends on the scale and effects of the act. The United States view is that the right of self-defense may be triggered by any unlawful use of force. The United States does not use a test of the gravity of the force, although proportionality would limit the lawful response. The policy argument for this approach is that a gravity test encourages actors to engage in small-scale uses of forces. The implication for cyber is that a framework that excludes states from taking responsive measures will not be



lasting. Cyber attacks that do not rise to use of force could still violate law, such as the law of sovereignty. States could take such violations to the U.N. Security Council, although there is some skepticism that the Security Council would respond in time given their slowness and the immediacy of cyber. A second way to react would be through law enforcement measures. A third way would be to use countermeasures. But, there is a question as to whether countermeasures will often be available, given the need to identify the perpetrator, the requirement to use countermeasures to induce compliance with international law, and that force cannot be used as a countermeasure. The concept of necessity for otherwise unlawful acts could be employed, although it is only available in exceptionally narrow circumstances. Ms. Perina concluded by remarking that international law must permit the reasonable use of force by states to protect their national security interests. Interdependence and interconnectedness may serve as a deterrence and incentive to create a stable and secure environment.

Professor Waxman analyzed the legal, strategic, and political dimensions of cyber attacks and armed self-defense. Initially focusing on the legal perspective, Professor Waxman stated that “armed attack” could be viewed as kinetic violence versus an effects-based or consequences-based analysis. But, there are difficult secondary questions related to proportionality, anticipatory self-defense, and state responsibility. Development is likely through state practice, not formal and global instruments. Turning to the strategic perspective, he noted that armed

self-defense to cyber attacks may be strategically valuable for protecting military and critical infrastructure through anticipatory or responsive military action, as well as for deterrence through credible threats. These strategic benefits must be balanced with strategic risks, including miscalculated escalation and eroding international norms prohibiting armed force. Finally, examining the third perspective, Professor Waxman stated the political context of cyber attacks will likely feature publicly ambiguous facts, high levels of secrecy, and challenges in proving attribution. Armed self-defense will likely require a high minimum threshold of harm to justify publicly. Very harmful cyber attacks are likely to occur in the context of other activities, such as hostile actions in the case of states, or criminal or terroristic actions in the case of non-states. He concluded by offering that there are a range of reasonable interpretations of cyber “armed attacks,” and a stable consensus is unlikely for the foreseeable future. Line-drawing near the margins is challenging for lawyers, but it may be less problematic in practice; states are unlikely to respond to small-scale, naked cyber attacks with force. The law can support strategy in calibrating appropriate triggers and thresholds for self-defense, but the unpredictable real-time political features of cyber attack crises make doing so in advance difficult.

Professor Gill discussed anticipatory self-defense. He began by defining self-defense as a long-recognized right states possess under international law to repel unlawful force and, if necessary, to overcome it. It is not maintenance of international peace and security, or



reactions to threats that have not yet materialized. The dual legal bases of self-defense are Article 51 of the U.N. Charter and customary international law. A temporal element has always been included, both reactive and anticipatory; reactive in the sense that force is being used to repel the current attack, and anticipatory in the sense that force is being used to forestall future attacks. Self-defense was placed in the U.N. Charter to integrate it into the Charter system, and to safe-guard the right of collective self-defense. There is a procedural reporting requirement when self-defense is used, and the state must put forth justification for its actions. When the right is invoked, a *prima facie* case must be made for defending oneself. Later, there is a second tier of reporting which requires a demonstration that the state remained within the parameters of necessity and proportionality. There are two questions for anticipatory self-defense. If anticipatory self-defense was part of pre-charter law, then at the time the charter was drafted, is there evidence that the drafters wanted to change this aspect of the law? This is a matter of the historical record, and there were references to anticipatory self-defense at the Nuremberg and Tokyo Tribunals. The second question is whether there have been changes to this right since then. He said the answer to this question is more problematic because there is a difference of opinion between states as to whether the right to anticipatory self-defense exists, and whether the pre-charter right is transferable or not. He believes there is an argument that it exists, at least as laid out in the *Caroline* case, that being immediate, overwhelming, leaving no choice of means

and no moment for deliberation. He also stated that preventive self-defense is not the same as anticipatory self-defense. Preventive self-defense is when there is some possible attack in the indeterminate future. This vagueness is not allowed for in self-defense. Professor Gill asked whether the rules should be changed for cyber. He answered that states must be allowed the tools and flexibility to allow states to act when there is no other feasible option. The crux of self-defense comes down to necessity. There must be necessity: an attack, with no other alternatives. Armed attack in cyber has two possibilities. First, it is a preparatory step for a kinetic attack; or second, it is used in isolation as a naked attack. The first possibility is much more likely. A series of small attacks, either cyber standing alone or in conjuncture with kinetic operations, could rise to the level of an armed attack, or a single, larger attack could be an armed attack. Cyber espionage, no matter how detrimental, is not an attack. There are no separate criteria for self-defense in the cyber domain than in the kinetic world. We may need to adapt or clarify certain rules, but we do not need new rules.

PANEL VI: Cyber Conflict and the Law of Armed Conflict

Colonel Gary D. Brown, USAF, the Staff Judge Advocate of U.S. Cyber Command, moderated Panel VI, consisting of Professor Michael N. Schmitt of the U.S. Naval War College, Professor Vijay M. Padmanabhan of Vanderbilt University,



and Major General Charles J. Dunlap, Jr., USAF (Ret.) of Duke University.

Professor Schmitt discussed classification of cyber conflict. He prefaced his remarks by stating that a new body of law for cyber is not needed. First, we need to figure out what the law is, and then apply the law to this new weapon. Professor Schmitt then addressed classification, a significant topic because classification of conflict is the first step in any law of armed conflict (LOAC) analysis. What type of conflict you are in determines what body of law applies: LOAC in its entirety, that portion of LOAC that applies to a non-international armed conflict (NIAC), or human rights law. The classic bifurcation is that an armed conflict is either international or non-international. Cyber operations take on the classification of the ongoing hostilities. Professor Schmitt then focused on a conflict in which only cyber operations are used. Common Article 2 requires an armed conflict between two or more states, and is generally accepted as customary international law. For an international armed conflict (IAC), there must be an “armed conflict” between two or more states. The duration and intensity of an armed conflict do not matter. “Armed” in the cyber context is any cyber operation amounting to an attack as a matter of law in the *jus in bello* sense. To determine if there has been an “attack,” look to the violent consequences, not the means employed. Death, injury, or destruction would be included, as would interference with functionality of an object resulting in damage. It does not include denial of service. But, if the operating system needs to be reloaded, that is damage, meaning it

was an attack, and therefore there is armed conflict. There could be an evolution of the standard to include massive economic disruption, or taking control of critical infrastructure in another state without damage or injury, but this evolution would be determined by state practice. The “international” requirement requires actions by the armed forces or other organs of a state so that it is state versus state. Private individuals acting in connection with the armed forces may be regarded as *de facto* state organs. If the state is in overall control of a group, that is sufficient, and if the group acts, it is as if the state had acted. There is a different standard if we are addressing an individual or a group of individuals who are not organized. Here, for the state requirement to be satisfied, there must be specific instructions by the state to the individual or group to conduct specific attacks. Groups acting on their own are not organs of the state unless the state subsequently endorses and encourages them. If a state merely tolerates attacks by others launched from its territory, it is not an IAC. But, it could be a breach of the obligation to police its territory. Turning to NIACs, Common Article 3 applies to a conflict not of an international character. The ICTY cites “protracted armed violence” between a state and an organized armed group or between two organized armed groups. Two requirements for a NIAC to exist are the intensity of the hostilities and whether there is an organized armed group. An additional type of NIAC exists for states that are party to APII; a NIAC could occur between a state and dissident armed forces that control territory. But, this excludes groups that only use cyber because they would not be able to control territory, so



this type of NIAC is not applicable to cyber and we can return to Common Article 3 NIACs. The first criterion is whether the group in question is organized. Different tribunals have defined “organized” using different terminology, but it is clear some degree of organization is required. It is not the same as “command responsibility.” It is sufficient to act in a coordinated manner, such as in mission planning and shared intelligence. It is a practical standard in which the acts are understood as those of the group, not individuals. This does not include individuals acting in concert, nor does it include individuals all accessing the same malware website. Next, Professor Schmitt turned to virtual groups formed on-line where the individuals do not know each other but act in a coordinated fashion and take orders from leadership. Professor Schmitt opined that these types of groups could meet the organized criteria. But, APII requires organized armed group to be under responsible command and have the ability to implement the Protocol. If this is a customary requirement, it would be difficult for a virtual group to comply with, and thus a group that is solely organized on-line could not fulfill the criterion. As for the intensity of the hostilities, APII excludes situations of internal disturbances and tension, such as riots, isolated and sporadic acts of violence, and other acts of a similar nature. This exclusion is customary international law. There is no bright line test. Some tribunals have cited the gravity of attacks, the collective nature, the need to increase forces to handle the conflict, and the duration. It is a high threshold that excludes highly destructive one-time

attacks, but the attacks need not be continuous. Summing up, Professor Schmitt said that cyber conflicts are possible in IAC, although the legal aspect of attribution for classification purposes could be difficult. They are unlikely in NIAC, because the level of required intensity would be hard to reach. But, expect the standards to evolve. We are not making new law; international law naturally evolves every day in areas other than cyber.

Professor Padmanabhan addressed cyber war actors. He described a scenario of an ongoing IAC or NIAC in which a cyber attack is launched, and a party to the conflict must decide whether to target or detain an individual who is believed to be responsible for the cyber attack. He then defined a combatant as being either a member of the armed forces of a party to the conflict, or, for a non-state group, either an individual who has a continuous combat function or an individual who is within the command structure of the organization. The Professor then displayed a chart laying out the lawfulness of targeting or detaining a lawful combatant, unlawful combatant, or civilian, and whether each in turn is entitled to prisoner of war privileges and combatant immunity. Turning to the NIAC between the United States and Al Qaeda, he examined five actors and analyzed their status in the conflict. He concluded by asking the difficult questions as he saw them. How should the United States use non-military personnel in cyber war? Is international humanitarian law the best body of law to handle hacktivists? What process must a state use to sort out



whether an individual is involved in cyber war given the variety of actors involved?

Major General Dunlap addressed command responsibility. He began by citing the *Yamashita* case, and commenting that, while some say that it stands for strict liability of a commander if war crimes are committed, the commission that tried the General seems to have concluded that he knew what was occurring under his command. In any event, what has evolved from that case and other command responsibility cases is that a commander's responsibility is predicated on a command relationship between a superior and a subordinate, information or knowledge that triggers a commander's duty to act, the requirement that the commander take some action regarding the subordinate's LOAC violations, and a causal relationship between the commander's omission and the subordinate's war crimes. Major General Dunlap then addressed the relationship between a commander and subordinate in cyber, and how that might impact adjudications of command responsibility. In particular, unlike traditional military operations, cyber operations may well be conducted by a mix-match of military personnel, civilians, government employees, and contractors. A commander cannot truly "command" these non-military actors, and he may not have the authority to punish them. Does the commander then actually command? He cited the *Taylor* case, in which the Special Court acquitted Taylor of the command responsibility charge. The court held that while Taylor had substantial influence over the actors, he did not have command and control. "Effective" command and

control over contractors and civilians is what must be shown, but a U.S. military commander cannot typically "command and control" contractors and civilians as he can uniformed subordinates. Turning to the second part of the test, the duty to act is triggered when the commander has knowledge of information that a LOAC violation is occurring. This could be difficult in the cyber setting. The case of *U.S. v. Calley* does stand for the general proposition that the subordinates who are passing an order can assume the legality of the order unless it is patently illegal. However, it is difficult to say that someone, even a commander, who is merely passing an order to conduct cyber operations would necessarily have the knowledge and expertise to appreciate that its outcome would be illegal. Next, he examined some other potential criminal charges for offenses related to cyber operations. Article 99 of the Uniform Code of Military Justice, for example, denounces Misbehavior Before the Enemy, and that offense criminalizes such actions as endangering the safety of a command through "neglect." He asked whether this could potentially be used against a commander for negligently failing to secure his command from cyber attack. Finally, ethical considerations were addressed, and the question was posed whether a cyber attacker has an obligation to identify himself. Is it perfidious if it looks like an uninvolved third-party state launched a cyber attack?



PANEL VII:

Cyber Attacks: The Law

Commodore Andrew Jameson, RN, Director of Naval Legal Services, moderated the final panel of the day, and introduced the panel as focusing on how international humanitarian law applies to attack in cyber. The panel consisted of University of Essex Professor Dr. Noam Lubell, Brigham Young University Professor Eric T. Jensen, and Air Commodore Bill Boothby, RAF (Ret.).

Dr. Lubell focused on military objectives in cyber attack. He began by observing that the dangerous ease in using the word “attack” has us believe that all cyber operations require analysis under LOAC. Many do not. If denial of service is an attack, then the legality of the attack depends on whether the website is a military objective. But, if denial of service is not an attack, the status of the website is irrelevant. A different approach is to say that cyber operations are more akin to psychological operations which do not cause deaths or significant damage. But, psychological operations do not cause direct harm to civilians, whereas cyber operations might, so the analogy is too sweeping an approach to always be appropriate. Most people would agree that cyber operations that result in casualties or significant damage could be classified as attacks. However, questions need to be asked as to the threshold of harm for it to be an attack, and whether it is necessarily physical harm. The functionality approach is a damage approach that has as its defining criteria the effect on the functionality of an object and if it needs to

be repaired with parts. A key question is whether the insistence on physical damage should remain part of the analysis. If significant and equal harm is caused without physical damage, should this not be an attack? As to the question whether data itself can be an object, although it is not “visible and tangible” it nevertheless is more of an “object” than an “objective,” and this was the key differentiation in the Protocol. The question of destroying data is interesting. Was the data destroyed if there is a back-up that can be retrieved? Buildings and cars that are destroyed can be rebuilt. So why is data destruction not an attack? In fact, the reason for excluding many of these operations from the definition of attack is in order to avoid categorizing minor inconveniences as attacks, but if the operation has a military objective as its target, then minor disruptions to civilians would likely be proportionate, and not unlawful. In addition, one needs to look at attacks in their entirety, not just the cyber operation in isolation, but the cyber operation as a component of a larger attack. Finally, he turned to examining whether certain industries could be targeted, such as a factory producing hardware or software. This could be analogous to a weapons factory if the hardware or software is clearly a military system. But, if the object only acquires its military character later down the road, then the factory is better analogized to a steel plant. He concluded by noting that a key concern for targeting is whether the operation will be an attack or not, which will trigger whether it is subject to distinction, and by questioning whether we need to rethink physical damage and find a new threshold of harm that would constitute an attack.



Professor Jensen spoke on precautions in attack and proportionality. He identified the threshold issue for the application of LOAC as being the definition of an “attack.” This is a hotly debated issue, but requires “acts of violence.” Civilians cannot be attacked, but there are things that can be done below the level of attack to achieve the desired aims. He then turned to the duty of constant care, and remarked that commanders cannot ignore the effects of cyber operations on civilians. Constant care must be taken to spare civilians. “Constant care” is not defined, but it must at least mean commanders cannot ignore the effect of their cyber operations on civilians. This provision applies to all cyber operations, not just cyber attacks, and requires a situational awareness for cyber operations. Next, he turned to proportionality. Citing Article 51 of the U.N. Charter, indiscriminate attacks are attacks which may be expected to cause incidental loss of civilian life, injury to civilians, or damage to civilian objects. It is more than just irritation, inconvenience, stress, or fear. He questioned whether damage to civilian objects would be triggered by damage to functionality. There is no prohibition on indirect effects, but only on indirect effects that should be expected. When considering indirect effects, a commander has to consider whether the cyber weapon could jump an air barrier from one network to another, and apply this as part of the proportionality analysis. The commander must be able to cancel or suspend the attack if the proportionality test prohibits continuing the attack. Turning to the feasibility standard, Professor Jensen stated that feasibility

applies to all precautions in attack. It is generally understood to mean those things that are practicable or practicably possible, taking into account the circumstances ruling at the time, and applies to both the tool and how it is used. If gathering information, such as mapping a network, is not practicable, then the attack should be called off because it would be potentially indiscriminate. However, because there are different standards of technology, the question becomes can a commander from a less technologically advanced state say there is a lower standard for them than a more technologically advanced state because certain precautions would not be feasible for the less technologically advanced state. The last topic addressed by Professor Jensen was precautions against the effects of attack. He said most states have said this is too hard, and try to explain this away. This is not a standard that waits for wartime, but must start long before hostilities exist. The responsibility to segregate military objectives from civilians and civilian objects must occur long before hostilities start. In the cyber realm, he asked whether the infrastructure could be segregated even if the traffic could not be. He also noted there is the responsibility to protect the civilian population and civilian objects from the dangers resulting from military operations. This does not apply to mere inconvenience or irritation. He asked what our response should be to the requirement to protect items under our control, and whether we should prepare a strategic cyber reserve of servers.

Air Commodore Boothby focused on weapons law. Means, he began, are the



weapons and weapon platforms, while methods are the ways the weapons are used. He first pondered how cyber could constitute a weapon. He analogized cyber to a rifle, and cyber attack to pulling the trigger on the rifle. A cyber weapon is any computer or computer device that can cause damage or injury to a person or object. Notions of use, intent, and design also need to be considered. While there can be numerous orders of effect following a cyber operation, damage or injury at any order of effect has the ability to render the cyber tool used a cyber weapon. If it is a cyber weapon, then certain things follow, like the application of weapons law. The *Nuclear Weapons* case tells us LOAC applies to all weapons, which would include cyber weapons. The right of the parties to an armed conflict to choose to use cyber weapons is not unlimited, and it is unlawful to use weapons of a nature to cause superfluous injury or unnecessary suffering. So, when looking at a cyber weapon, we compare the nature and the scale of the generic military advantage to be expected from use of the weapon, and look at the pattern of injury expected by its normal use. But, usually, a cyber weapon is designed for a specific operation or target. So, *ad hoc* circumstances must be considered when applying this test. Air Commodore Boothby then addressed the other customary law principle applying to the use of weapons, the prohibition on weapons that are indiscriminate by nature. This is particularly potentially relevant in the case of cyber weapons, the critical issue being whether the cyber weapon limits the damaging effect reasonably to the intended target. We must consider certain types of worms, viruses, and

malware that spread their damage uncontrollably. Planning cyber attacks is going to place demands on intelligence resources. There is a prohibition on weapons or means of warfare that are intended or may be expected to cause widespread, long-term and severe damage to the natural environment; while the United States is not a party to this convention, U.S. allies are. Second and third order effects must be examined to determine if the rules are relevant. He then turned to the Convention on Conventional Weapons (CCW), and examined taking control of air-borne vehicles armed with incendiary weapons, noting that a state that did so and that is party to Protocol III to CCW would need to comply with its rules in any use of the incendiaries. He stated it would probably be unlawful to take control of a laser by cyber means and adapt its combat function to causing permanent blindness. He turned next to booby traps, such as a cyber kill switch planted by malware and placed on a computer system. It is only a booby trap if it is designed to kill or injure. What if the kill switch is designed to disable the electrical supply to life-support activities? He said a national interpretation is required. What about a thumb drive bearing malware as the delivery system: is the cyber weapon the malware or the thumb drive? He opined that again a national interpretation is required. Turning to weapons reviews, reviews are required of both cyber and non-cyber weapons. Operations lawyers are likely to need to perform weapons reviews of cyber weapons as well as giving targeting advice for specific operations. Legal review of all cyber weapons should also be done generically. If a network of computers



sends spam to a targeted system for denial of service, that may not be a cyber weapon. But, if the targeted system provides life support systems, and death or injury to protected persons is likely as a result of that denial of service, a weapons review would be necessary. He then addressed a masquerade cyber tool whereby users are diverted and malware is installed. It is only when death or damage are expected that it becomes a cyber weapon. But how do you comply with the indiscriminate weapons prohibition if it affects all visitors? It is important to know who is using the targeted system, whether civilians or military personnel. The ability to control, monitor, and even reverse cyber effects will become more of an issue in the future.

PANEL VIII:

Beyond International Armed Conflict

Panel VIII began the final day of the conference, and was moderated by Captain (N) Geneviève Bernatchez, Office of the Judge Advocate General, Canada, and consisted of Professor Robin Geiss of the University of Potsdam, Professor William C. Banks of Syracuse University, and Dr. Jann K. Kleffner of the Swedish National Defense College.

Professor Geiss began the panel with a discussion of non-international armed conflict (NIAC) and cyber warfare. He first posited whether the subject was topical. All of the headlines have an interstate character. But, cyber operations will show up more and more in NIAC. The first question is whether a non-state NIAC

having resorted only to cyber can trigger an IAC. He answered only in very rare situations. There is a necessary threshold of violence, and an organized armed group is required to participate in the hostilities. Individual hackers sitting at home are not an organized armed group. Against this background, virtual groups will not qualify as an organized armed group. A virtually organized group could not come close to the level of organization required, and deciding who is a member of the group would be difficult. If there were continuous attacks, the machines involved could eventually be discovered, but a long period of time would be required to discover the identities of the people involved. The next question is what happens if cyber operations occur in an ongoing NIAC. There is no prohibition on the use of cyber operations. There could be a lot of potential for cyber operations if cyber vulnerabilities of non-state actors could be identified. Some problems that stem from technology are its artificiality, its interconnectedness, and its global connectedness. Professor Geiss concluded by noting that necessity could be a useful legal mechanism in the cyber domain, used when attribution is lacking. If there is attribution, countermeasures could be used.

Professor Banks spoke to counter-terrorism responses to cyber attacks. He began by asking whether counter-terrorism law provides a useful supplement or bridge to LOAC for responding to cyber intrusions when there is no armed conflict or when the cyber operations are not part of a larger kinetic operation. Cyber terrorists use internet-based attacks for terrorist attacks, including acts causing



deliberate, large-scale disruption of computer networks. To qualify as a cyber terrorist attack, an attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Although the definition of terrorism has been in play, the question is whether counter-terrorist law provides a useful legal paradigm for cyber terrorism. The elephant in the room is the problem of attribution. Attribution could be aided by forensic tools, but it is not always fast and not always certain. Whether dealing with state or non-state adversaries, the *ad bellum* authority to use military force is tied to attribution of the attack and thus identification of the enemy. One starting point for addressing *ad bellum* authority is addressing the consequences. Cyber intrusions can range from the trivial to the devastating. What legal framework is used determines permissible responses to cyber terrorist attacks where there is no ongoing armed conflict that causes physical damage but where there is wide-spread and considerable economic harm, such as an attack on a stock exchange. Is that destruction of property a sufficient trigger for a counter-terrorism response? The answer, Professor Bank stated, turns in part in whether the state wants to use force in response. The Professor therefore addressed countermeasures, and said they are temporary, lawful actions undertaken by an injured state in response to another state's internationally wrongful conduct. He questioned whether they were lawful against non-state actors such as terrorists, and answered maybe. Customary law permits state responses to violations, such as the norm of non-intervention, to acts that do not rise to the level of an armed

attack. Little has been said regarding countermeasures, including active defenses, which call for an in-kind response to disable the source of the attack while it is underway. Active defenses are a sub-set of reciprocal countermeasures where the injured state ceases to obey the same norm the other state has violated. Active defenses may deploy electronic force only when force is authorized. Would counter-terrorism law provide an answer to the tautology of that analogy, meaning that you can use force only if it is determined that force has been used against you? He asked whether counter-terrorism law could answer this and provide some authority to that which is necessary. Countermeasures are complicated by the issue of attribution, but they must be costly enough so as to discourage the intrusion. Countermeasures could be less effective against non-state actors because those actors could simply relocate. If a cyber attack constitutes an armed attack, self-defense allows the victim state to conduct forceful operations wherever the terrorists are located if the state in which they are located is unable or unwilling to police its own territory. The framework of counter-terrorism law relies on LOAC, human rights law, refugee and asylum law, and criminal law together with the U.N. Charter; however, there is currently no coherent international legal regime covering terrorism and its responses. Summing up, Professor Banks commented that many in the international community are understandably critical of U.S. law's path. But, the critique of counter-terrorism law as a product of U.S. domestic law could be misplaced. Norms of counter-terrorism law could support the



way forward. More than just an extension is necessary; new norms in *ad bellum* may be needed, at least at the margins. The law is not mature and cannot leap ahead of strategy and policy.

Dr. Kleffner focused on the international legal aspect of cyber operations in relation to peace operations. His discussion pertained to all peace operations, not only traditional peace keeping operations that are governed by the three core principles of consent, impartiality, and the use of force in self-defense, but also peace enforcement and peace building operations. First, he said, one must determine the applicable law that governs peace operations and cyber operations in the course of peace operations. One must distinguish between cyber operations that are below the threshold of an armed conflict, versus those that are above that threshold. Below the threshold, international human rights law (IHRL) is the governing framework. States are bound by conventions and customary law, provided there is jurisdiction. Similarly, international organizations are bound by customary IHRL. Therefore, if and when an international organization exercises effective control over territory, or control over one or more persons, the international organization is bound to respect the human rights of those who find themselves in its jurisdiction. For cyber operations that are below the threshold of an armed conflict, there must be a concern for such rights as privacy, freedom of speech, and the like. The application of IHRL broadly turns on jurisdiction, meaning effectively control. But, cyber operations can be carried out remotely, making it difficult to see how IHRL applies to peace operations below

the threshold when there is no exercise of jurisdiction. In order to avoid a legal vacuum, we might need to adapt an effects based approach to jurisdiction for IHRL to apply. There may have to be an adjustment in the legal framework due to the unique characteristics of cyber operations. A second issue is the protection and loss of protection of peace personnel and equipment; this issue arises when the peace operation is occurring above the threshold for an armed conflict. However, peace operations that amount to an armed conflict are rare. Usually, the peace operation is operating between parties to an armed conflict. The peace keeping party itself is not participating in the hostilities. But, the party will become subject to LOAC if and when they become a party to the armed conflict. The third issue is of responsibility. It is important to identify who the relevant actor is. The question is one of attribution; decide who is acting, then determine responsibility. For the question of attribution in peace operations, the decisive factor is whether the U.N. Security Council retains control. The mere fact that a peace operation in a particular state is due to a Security Council resolution makes it attributable to the United Nations. Does that automatically exclude responsibility of the third country national? Sometimes it does, but more than one entity can have responsibility.

PANEL IX: The Road Ahead

Professor Dennis L. Mandsager of the U.S. Naval War College moderated the final panel of the conference, consisting of Brigadier-General Kenneth W. Watkin,



OMM, CD, QC (Ret.) of the U.S. Naval War College, Dr. Cordula Droege of the International Committee of the Red Cross, and Professor Michael J. Glennon of the Fletcher School of Law and Diplomacy, Tufts University.

Professor Watkin focused on self-defense. He began by commenting that the road ahead is still being paved. The tarmac has not solidified. He then commented that there are some terminology issues. He claimed to be a cyber skeptic because of the Y2K non-event, despite predictions of disaster. But, much has changed since Y2K. Cyber is here to stay. Over thirty countries have a cyber unit in their military order of battle. Cyber is a challenge shared across government and across governments. This first challenge is the prevalent and predominately non-military use of cyber in society. The second challenge is the dialogue unfolding in international law with what is fundamentally a micro-force. He then commented that the cyber domain is a national asset, and asked whether only the military will defend it. Nations seem more focused on cyber crime, identity theft, and economic security, and the military is usually at the back of the policy. What really is defense, and what really is the threat? Law enforcement could be a possible predominate notion, more so than armed conflict is. Most citizens are more worried about on-line shopping than about armed cyber attack, and that will ultimately frame how governments look at this issue from a security perspective. We compartmentalize, keeping *ad bellum* separated from *in bello*, and international humanitarian law from international human rights law. One challenge is

domestic law. The talk regarding domestic law is of authorizations, but it is more relevant to discuss restraint and keeping control of this cyber beast. Another challenge is an expansive notion of the home front. This calls for a true application of operational law for all operations, not just the application of LOAC. This may be a doctrinal and training challenge for operational lawyers. The *lex lata* is important. It is a myth that the *lex lata* is all that clear. Looking at missile warfare, by analogy, treaty law is hard to find and what you get is very learned documents and points of view of what the law is or what the law should be. This requires us to broaden our horizons. Professor Watkin then turned to weapons, which raises issues of *de minimus*. Is the effect of having to reload software an attack? As hardware gets smaller, we have to convince others that the threat is getting bigger. Another challenge is classification. Who knows how to talk cyber? The challenge is having the right lawyers around the table. Also, where are the human rights committees? Governments have tremendous power, but who is regulating the governments? Turning to *jus ad bellum*, we use the same words, but not the same language. We talk about thresholds like they are written in stone. But, the old rules were written for the old conflicts. We now have an old leash on a 21st century beast. We live in a more and more complex world. What is the threshold for grave and less grave if someone takes over an electrical system? What will be the standard to go to war? There is a state reluctance to create new international humanitarian law. States like constructive ambiguity. The question is how to put a framework around the



technical advances that we have had. He then turned to the notion of reciprocity, and commented that the notion of grave and less grave will have some fluidity. So, we wait until states scare themselves into creating a new framework. Professor Watkin hopes the human rights community will get more engaged on the stage. Perhaps states will talk to each other more. We must ask the techies whether they are sure about collateral damage and whether things will turn out the way they think.

Dr. Droege spoke to *jus in bello* in international humanitarian law (IHL). She stated that there is clearly no agreement regarding the adequacy of IHL in terms of cyber warfare. The two sides of the argument are that we should be cautious applying IHL to cyber, versus IHL is used to seeing new weapons and cyber is just another weapon. As for the first argument, urging caution, it is said that we should ban new weapons such as cyber before there is a catastrophic incident, and that we are in need of a new treaty regarding cyber warfare. The political appetite is to not go down this road for a new treaty. From a strict IHL view, it does envision new weapons as it calls for weapons reviews. She asked what rules in IHL would stop a party from fighting a war effectively? What are the gaps, or are there gaps, in protecting the civilian population? There can be specific gaps that regulate in one area, but not in another. For the rules for cyber and the conduct of hostilities, the rules are well known. There are two potential gaps: first, in the possible interpretation of rules, and second, when weak rules are exasperated for new circumstances. It can be strength

of the legal framework to say the rules can be interpreted for new situations, but it can also be a weakness if there is not enough protection. The crucial question in *jus in bello* armed attacks is deciding what is an armed attack. LOAC does not protect civilians from being left alone, but protects them from being harmed. Another potential normative gap in the protection of civilians is if the interpretation is exasperated for cyber warfare. One gap here applies to dual-use infrastructure. Some such infrastructure is more vulnerable to remote cyber attack than from kinetic attack. Most if not all of cyber space is dual-use. The principle of distinction will not be the most protective principle in this effect, since we turn quickly to proportionality. This principle is notoriously vague and relatively weak. Another example is the definition of a military objective. For some, war sustaining could include financial systems. This creates a normative gap for the protection of the civilian population. In terms of general rules, it is difficult to say we have clear gaps. It is not clear where the gaps might lie, as the states have left ambiguity.

Professor Glennon posited whether there are gaps in the law, and, if so, what is the likelihood that the international law regulating these matters will be tightened up. He began by stating that one might conclude that there are no gaps. It is only a matter of finding the right category. The process of finding the answer is going through the decision tree from one category to the next and coming to the correct conclusion. This approach to the law has been described as fundamental legalism. His response is that categories



are not all there is to law. A good lawyer does not look only to classification, but also to the purpose behind the category. It must be asked whether the category is still relevant, and the policy behind it must be examined. The structure of incentives and disincentives that will occur by interpreting a rule one way or the other should be considered. It is much more complex than merely performing categorization. Categorization provides an illusionary certainty. He argued that this light switch approach of either being on or off is wrong because there can be a third choice, which is to say that the law does not provide an answer. Reasonable people can differ as to whether the categories apply. International law has a default when there is a gap, and it is called the freedom principle. A state will be deemed to be free to act unless another state meets the burden of persuasion that there is some prohibition. Professor Glennon then addressed a second question: is it likely that the law is moving in a direction in which greater restraints are being placed on states? He answered there is some reason to hope if you believe that restraints should be tightened. But, the goal of greater legal tightness must be identified. Prevailing conditions offer a shadow of the future. However, if you do not know who the actor is because of covert operations, there can be no shadow of the future. If actions are overt, then they are more likely to be known. Another issue is the ability to penalize offenders, which is highly improbable given issues of covert operations. Professor Glennon concluded by remarking that there are various scenarios of how the law develops depending on which conditions prevail. There is a good probability of the

continuation of the process that we are currently in of attack and response. He characterizes this as a drip, drip war, or perpetual cyber war, resulting in more and more strikes based upon weaker and weaker evidence.

KEYNOTE ADDRESS:

Professor Yoram Dinstein **Professor Emeritus, Tel Aviv** **University**

Professor Dinstein, the 1999/2000 and 2002/2003 Stockton Professor of the U.S. Naval War College, delivered the closing address. He stated that he was bothered and bewildered by the conference. Much of the discussion had nothing to do with war. Yet, he said, the theme of the conference was supposed to be cyber war, and war is the real challenge in this field. Issues such as sovereignty are largely a diversion. The sovereignty of the enemy is ignored in wartime. Sovereignty is then relevant only in the context of neutrality.

As far as the *jus ad bellum* is concerned, it is not enough that a cyber operation reach the level of the use of inter-State force (prohibited by Article 2(4) of the U.N. Charter). The paramount question is whether the operation amounts to an armed attack (which is a condition precedent to the exercise of self-defense under Article 51 of the Charter). Absent an armed attack, the target state has only three choices: 1) it can go to the Security Council; 2) it can use countermeasures, or 3) it can sue (assuming that there is a court vested with jurisdiction). There is a gap between use of force (Article 2(4)) and an armed attack (Article 51). All the same, the gap is not very wide, and it was



wrongly exaggerated by the International Court of Justice in the *Nicaragua* judgment of 1986.

Professor Dinstein was surprised that some people failed to appreciate that cyber electrons can cause an armed attack. He stressed that a computer can be used as a weapon. The test is not what a weapon looks like but what harm it can produce. In fact, the use of a computer as a weapon may cause fatalities on a large scale by bringing about the crash of an aircraft; by starting a flood through the opening of the sluices of a dam; and even by causing a meltdown in a nuclear reactor.

Professor Dinstein then addressed the issue of attribution, and pointed out that the problem occurs in kinetic no less than in cyber warfare. He cited the *Corfu Channel* case of 1949, in which the International Court of Justice failed to determine which particular state had laid naval mines that exploded in international straits. In his opinion, attribution is usually possible: it is only a time-consuming process. At bottom, there are two options for a cyber attack. It can be either an isolated event or a precursor to other attacks. If an isolated attack, there is all the time in the world to figure out who perpetrated it. If a precursor to a stream of other attacks, the identity of the attacker will be soon established anyhow.

The response to a cyber attack can be kinetic, just as the response to a kinetic operation can be by cyber. We have to simply apply to cyber warfare the general principles and rules of the *jus in bello*. Contrary to what has been suggested by

some speakers, the main core of the LOAC *lex lata* is not in doubt.

He traced some of these basic principles. First, direct attacks against civilians or civilian objects are prohibited. It follows that direct attacks against civilian computers are forbidden. The problem is that we do not always know if a computer is civilian in character. Admittedly, in case of doubt, we must assume that a computer is civilian. However, this depends not only on the hardware but also on the software actually stored in it. Any computer which is designed as a part in a weapon system is military by nature. But even a run-of-the-mill computer employed by the military for the most mundane administrative purposes is military by use.

The second principle is the injunction against indiscriminate attacks. If a destructive virus is planted in a military computer, but the virus can spread uncontrollably to civilian computers, this will be regarded as an indiscriminate attack. There is no difference in this context between a virtual virus and a biological virus.

Third is the crucial subject of collateral damage and the interlinked principle of proportionality. The trouble is that proportionality is a matter of evaluation and judgment. In the final analysis, two persons or two states may disagree as to whether the collateral damage ensuing from a specific attack against a lawful target was expected to be excessive compared to the military advantage anticipated. The linchpin on which proportionality hinges is reasonableness. Still, it is important to keep in mind that



2012 Naval War College International Law Conference Brief

the outlook must be holistic. If a whole array of computers is under attack, the military advantage must be assessed on the basis of the entire operation, rather than any segment thereof.

Professor Dinstein concluded by addressing two final issues. First, LOAC is not applied to cyber attacks by analogy. It is applied directly. Hence, a cyber operation is an attack only if it entails violence. It follows that a mere disruption or discomfort is not an attack. Even

espionage is not an attack. In any event, espionage *per se* is not unlawful for States. Only the individual spy may be subject to prosecution if caught in the act.

Second, the more cyber you have, the more vulnerable you become to a cyber attack. A state with no F-15s or aircraft carriers can take down the United States with cyber. So, in his view, the top priority of Cyber Command should be to war-game the scenario of a cyber Pearl Harbor.