Penn Law
UNIVERSITY of PENNSYLVANIA LAW SCHOOL
Center for Ethics and the Rule of Law

Definitions and Foundational Concepts:

- Cyberspace:
  - "The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." (Unclassified definition from NSPD-54/HSPD23).
  - Coined by the science fiction author William Gibson in *Neuromancer* (1984); layman's terms related to Information Warfare (IW): *cyber medium, infosphere, datasphere, virtual realm,* and *virtual battlespace*.
  - RAND's "...global world of internetted computers and communication systems" (Hundley 1994).
  - Involved organizations include: the Internet Corporation for Assigned Names and Number (ICANN), which coordinates the IP address space and Domain Name system; the Internet Engineering Task Force (IETF), which develops technical standards that various networks voluntarily adopt; and the Internet Governance Forum (IGF), which meets to discuss the future of internet governance.
  - There are four main modes of internet regulation: (1) the law of individual governments, (2) internet architecture, which determines how information can be transmitted; (3) norms and inherent community standards, which often leading to self-censorship; and (4) markets (Lessig 1999).

- Cyberwar:
  - A/k/a Cyberspace Operations - The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (Joint Pub 1-02 2011).
  - Arquilla and Ronfeldt (1993) use "cyberwar" to designate 'knowledge-related conflict at the military level' and limit their application of the term to IW strategies "...of the sort that might be used against insurgents by a high-technology opponent..." (cited in Morton (1995)). For these authors, cyberwar is contrasted with *netwar* (taken in the sense of non-military information warfare).
  - A synonym for *information warfare* (Grier, 1995)
  - In contrast, the term is also used as a synonym for *netwar* -- a superset of (IW)(Szafranski, 1995).
  - Libicki (1995) calls cyberwar "combat in the virtual realm."

- A non-exclusive list of some *early* and *known* cyberwarfare incidents (Strategic Cyber Security 2011):
  - 1999: unknown Serbian hackers try to disrupt NATO military operations;
  - 2007: Syrian air defense was reportedly disabled by a cyber attack moments before the Israeli Air Force demolished an alleged Syrian nuclear reactor; massive cyberattacks experienced by Estonia, with most of the compromised and attacking computers located within the U.S.;
  - 2008: Russo-Georgian war with integrated cyber and conventional operations;
  - 2009: the whole of Kyrgyzstan was knocked offline during a time of domestic political crisis;
  - 2010: Stuxnet worm, reportedly launched by US against Iran , identified as most sophisticated state-sponsored malware.

Status of Cyberwar in the Law of Armed Conflict

- "The United States has affirmed that established *jus ad bellum* rules do apply to uses of force in cyberspace … The inherent right of self-defense potentially applies against *any* illegal use of force…there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response. [Not every] illegal use of force triggers the right to use any and all force in response – such responses must still be *necessary* and of course *proportionate*." (Koh DoS 2012).
- "At least one country [China] has questioned whether existing bodies of international law apply to the cutting edge issues presented by the internet. Some have also said that existing international law is not up to the task, and that we need entirely new treaties to impose a unique set of rules on cyberspace. But the United States has made clear our view that established principles of international law *do* apply in cyberspace." (Koh DoS 2012).
- The "Tallinn Manual" (2013) will be "the first of its kind to attempt to delineate the threshold dividing cyber war from cyber crime and formalize international rules of engagement in cyberspace."

Are Offensive Uses of Cyberweapons Justified for National Security?

- "If a cyber attack results in a level of human suffering or economic destruction equivalent to a conventional military attack, then it could be considered an act of war, and it should be subject to the existing laws of war." (Strategic Cyber Security 2011).

- "[E]ach [People's Liberation Army] military unit has a clear, offensive cyber mission in times of both war and peace. In peacetime, strategic intelligence is gathered via cyber espionage to help win future wars." (Strategic Cyber Security 2011).

Cybersecurity, Privacy and Police Powers

- The continued success of the Convention on Cybercrime requires addressing myriad national and international data security and privacy concerns, including respect for national sovereignty (Strategic Cyber Security 2011)
- National sovereignty and data privacy concerns would have to be carefully guarded with any future Cyber Weapons Convention (Strategic Cyber Security 2011).
- Privacy must be balanced with legitimate law enforcement powers, but the mere creation of an international platform would enhance cyber security and freedom of expression. (Strategic Cyber Security 2011).
- "Cyberspace significantly increases an actor's ability to engage in attacks with "plausible deniability," by acting through proxies … effects, dual use, and attribution are difficult legal and policy questions that existed long before the development of cyber tools." (Koh DoS 2012).
- Major laws impacting internet privacy include but not limited to: Gramm-Leach-Bliley Act (1999), allowing personal information to be transferred between joined companies; the Homeland Security Act (2002), joining 22 federal agencies together under the Department of Homeland Security and mandated the establishment of an Privacy Officer to ensure individual privacy rights are respected; the Intelligence Reform and Terrorism Prevention Act (2004), promoting interagency cooperation, sets up Privacy and Civil Liberties Oversight Board.

Cyberwar and International Humanitarian Law

- "[The U.S. sees] law not as a straitjacket, but as one great university [Harvard] calls it when it confers its diplomas, a body of "wise restraints that make us free." International law is not purely constraint, it frees us and empowers us to do things we could never do without law's legitimacy." (Koh DoS 2012).
- "[N]ational security planners have no time to waste in reevaluating, and updating, if necessary, the Geneva, Hague, and Human Rights conventions, as well as the Just War theory, and more." (Strategic Cyber Security 2011) (e.g.,"Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land." The Hague, 18 October 1907; ICRC Interpretive Guidance On the Notion of Direct Participation in Hostilities, 2009.
- Challenges of "Political will, Universality, Assistance, Prohibition, Inspection" regarding any new cyber treaty (Strategic Cyber Security 2011).
- "We talk *openly and bilaterally* with other countries about the application of established international law to cyberspace …*multilaterally*, at the UN Group of Governmental Experts and at other fora, in promoting this vision of compliance with international law in cyberspace …*regionally*, as when we recently co-sponsored an ASEAN Regional Forum event to focus the international community's attention on the problem of proxy actors engaging in unlawful conduct in cyberspace. Preventing proxy attacks on us is an important interest …we have outlined the ways that existing international law addresses this problem." (Koh DoS 2012).

Cybersecurity and the Private Sector

- "Cybersecurity [is] one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter;" 12 initiatives proposed "To establish a front line of defense against today's immediate threats," "To defend against the full spectrum of threats," and "To strengthen the future cybersecurity environment." (CNCI 2012).
- The U.S. acceded to the Council of Europe Convention on Cybercrime on January 1, 2007; China, Russia, Tajikistan and Uzbekistan submitted International Code of Conduct for Information Security to the UN 2011.
- The new "language" of networks, Internet Protocol version 6 (IPv6) stellar number of viable computer addresses and its enhanced security features will have adverse effects on individual privacy and online anonymity during the long transition period from IPv4 to IPv6[;] hackers will be able to exploit vulnerabilities in both languages at once (Strategic Cyber Security 2011).
- Information and communications infrastructure is often shared between State militaries and private, civilian communities. The law of war requires that civilian infrastructure not be used to seek to immunize military objectives from attack, including in the cyber realm (Koh, DoS, 2012).
- "[C]ybersecurity, cybercommerce, fighting child pornography and other forms of cybercrime. stopping intellectual property piracy, as well as promoting free expression and human rights [are issues aside from] cyberconflict [which do] not constitute the whole of our approach to cyberspace; they are an important part – but only a part –of this Administration's broader "smart power" approach to cyberspace." (Koh, DoS, 2012).