Cyberweapons and cyberwarfare have become the most dangerous innovation of this century\(^1\), and are now considered by the FBI to be the number one threat ahead of terrorism.\(^2\) Cyberweapons bring peril to economic, political, and military systems by a single act, or by multifaceted orders of effect, creating a dreadful new total war potentiality in every dimension. Cyber-attacks put immense pressure on conventional notions of sovereignty and the moral and legal doctrines that were developed to regulate them. Unlike past forms of warfare circumscribed by centuries of just war tradition and law of armed conflict prescriptions, cyberwarfare brings new areas of ambiguity, including violation of third party sovereignty, the use of cyber attacks by non-state actors acting independently or in concert with states, and the timing, manner, place, and consequences of cyber attack that could be interpreted as acts of war.\(^3\) These legal ambiguities, in the void of moral perspective, make adherence to the rule of law a more challenging concept than in any other domain of warfare.\(^4\)

In the United States, cyberwarfare technology was originally developed by the Bush Administration and the Obama Administration has further expanded its use. While Secretary of State Clinton has claimed that such tactics are used against al Qaeda\(^5\), the use of advanced techniques in cyberwarfare is most evident in recent operations against Iran. The United States

---


\(^4\) Id.

purportedly developed a data-mining virus called Flame, a reconnaissance virus named Duqu and a computer worm dubbed Stuxnet that interrupted Iran’s nuclear program by attacking industrial control systems and causing Iranian centrifuges to spin out of control. In doing so, the United States has for the first time used computer programs for an end which until recently could only be achieved through bombs and other conventional weapons. These actions by the United States will not likely be the last cyber attacks as the Pentagon’s Defense Advanced Research Projects Agency (DARPA) has recently funded Plan X, which has the goal of not only protecting computer systems but developing the capabilities to disrupt or destroy enemy systems.

The United States and its allies are hardly the only world powers that have been developing a cyberwar capacity. In 2007, security firm McAfee estimated that 120 countries had already developed ways to use the Internet to target financial markets, government computer systems, and utilities. In 2008, the Russian government allegedly integrated cyber operations into its conflict with Georgia. According to these accusations, Russian cyberintelligence units conducted reconnaissance and infiltrated Georgian military and government networks. When the conventional fighting broke out, Russia used cyberweapons to attack Georgian government and military sites as well as communication installations. Foreign militaries, such as China’s, have conducted exercises in offensive cyber operations, both stealing information from other governments and simulating attacks on other countries command and control systems. In 2011, Iran boasted of having the world’s second-largest cyber-army. With states around the globe improving their cyberwarfare capabilities, the world may experience a cyber arms race reminiscent of the Cold War’s nuclear arms race.

The right time to explore the ethical and moral issues that surround cyberwarfare is before the issues becomes politically charged and overly emotional. Moreover, exploring the issues of cyberweapons now offers the chance to be proactive and gain an understanding of the ethical and legal issues of cyberwarfare before irreparable mistakes are made. For example, the new cyber-reality threatens traditional notions of sovereignty. When a state engages in traditional methods of military force, there are well-defined doctrines to determine when an attack infringes on another state's sovereignty. These questions are important because they helped determine when an attack has occurred that is sufficient to trigger a defensive response. But when a state engages in a cyber-attack, when and how do we determine that the attack has infringed upon another state's sovereignty? After all, no physical assets such as tanks or bombs have crossed physical boundaries (thus violating a state's territorial integrity in the
conventional sense), yet the results of the attack are often undeniable, as was the case with the Stuxnet worm launched against the Iranian nuclear program. Should we use an effects test? Furthermore, does a cyber-attack trigger a right of cyber-defense, or is a traditional military response allowed? Cyber-attacks put immense pressure on conventional notions of sovereignty and the moral and legal doctrines that were developed to regulate them. In a world of attack and destruction without conventional military assets, do traditional notions of sovereignty based on geography and territorial integrity retain their relevance?

This conference will assist in proactively addressing the ethical and moral issues that surround cyberwarfare by discussing whether the Laws of Armed Conflict apply to cyberspace just as they do to traditional warfare. If they do, then under what conditions does a cyber attack amount to an act of war? What is a proportional response to a cyber attack? Likewise, the conference will also discuss legal questions such as whether the U.N. Charter, which promises that members will not use the “threat or use of force against the territorial integrity or political independence of any state” (Article 2, Section 4) is inadequate with increasing use of cyberattacks. This leads to questions of whether problems of cyberwarfare require new treaties and legal definitions. For example, does the cyber race require treaties similar to the Treaty on the Non-Proliferation of Nuclear Weapons? To address such questions and more, this conference seeks to bring together leading authorities in the law, technology, and ethical philosophy. By better understanding these ethical issues now, we can be better prepared as cybersecurity becomes a more integral aspect of national security.