Mr. Clarke pointed out the diversity of cyber issues impacting the daily lives of ourselves and our country - e.g. stores hacked, countries attacked, phones seized, etc. He laid out a simple typology for helping us make sense of these myriad stories, organized around the acronym “chew.” Chew stands for Crime, Hacktivism, Espionage, War.

Cyber crime involves the penetration of computer networks to steal money from entities such as banks and companies, with these crimes perhaps amounting around the globe to two billion dollars annually.

- An example of such a heist is a thief getting into a company’s network, assuming an employee’s identity, generating a phony bill, and then wiring payment to himself.

These operations often cover vast distances, with many originating in countries such as Russia, Ukraine Belarus, Vietnam, Romania and Bulgaria. Criminals in these cyber sanctuaries are rarely pursued, as sometimes government officials are in on the take from this lucrative business.

The second category, hacktivism, combines computer hacking with politically motivated crusading. Hacktivism involves breaking into a network, stealing confidential information, and posting that information publically. The aim is to embarrass and constrain the stolen documents’ originator. A perfect example is Edward Snowden stealing and making public secret NSA materials.

- One impact of the Snowden revelations has been that U.S. opponents, including terrorists, have learned how NSA collects information, and have adapted their behaviors to make that collection more difficult.

The third category of cyber operations is espionage. In the past, espionage was dangerous - approaching foreign nationals to attempt to recruit them to spy against their countries. Not so anymore. Essentially all U.S. Agencies and Departments have been breached by cyber spies operating from a distance. Espionage is not just against government entities; private companies, for example, are targeted for the theft of valuable intellectual property.
• Seventy percent of major companies hacked were unaware until the U.S. government informed them, and the length of time it took for them to learn of an incident was about \( \frac{3}{4} \) of a year. China seems to be the main perpetrator of this type of cyber espionage. China will steal anything of value (e.g. contract bids, stock market tips, etc.), including costly R&D work.

The fourth category is war. Much like bombs, cyber war involves the physical destruction or disabling of a facility or grid. This is accomplished by inserting computer code that allows an attacker to assume control of the system.

• Last year in connection with the confrontation with Russia, Ukraine’s power grid was remotely shut down and the computers that could have served to restore service were destroyed.

The Internet of Things refers to 5 billion devices globally (moving toward 50 billion) talking to and interacting with each other. Everything is increasingly connected, and everything that is connected can be attached. Clarke emphasized that this is not science fiction.

• Five years ago the United States established a warfighting Cyber Command. Today, 26 nations admit to having such an organization.

Clarke characterized the U.S as good on offense, and weaker on defense. So, what can Americans do to guard against the cyber risk?

• First, our educational institutions need to train more graduates in how to defend computer networks. There are hundreds of thousands of job openings for well paying information security analysts.

• Second, we should seek an expansive official policy of cyber protection - to include not just government, but also corporate America, and citizens as well.

Paul F. Herman, Jr.
Florida State College at Jacksonville