गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

राष्ट्रीय न्यायिक विज्ञान विश्वविद्यालय
National Forensic Sciences University

Unit-4 Cyber Warfare-II



Dr. Lokesh Chouhan

Associate Professor

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

राष्ट्रीय न्यायालयिक विज्ञान विश्वविद्यालय
(राष्ट्रीय महत्त्व का संस्थान, गृह मंत्रालय, भारत सरकार)
National Forensic Sciences University
(An Institution of National Importance under Ministry of Home Affairs, Government of India)

E-Mail: Lokeshchouhan@gmail.com, Lokesh.chouhan_goa@nfsu.ac.in

Mob: +91-898924399, 9827235155

Reasons for Cyber War

- business' financial details
- customers' financial details (eg credit card data)
- sensitive personal data
- customers' or staff email addresses and login credentials
- customer databases
- clients lists
- IT infrastructure
- IT services (eg the ability to accept online payments)
- intellectual property (eg trade secrets or product designs)

- Cyber attacks against businesses are often deliberate and motivated by financial gain. However, other motivations may include:
  - making a social or political point - eg through hacktivism
  - espionage - eg spying on competitors for unfair advantage
  - intellectual challenge - eg 'white hat' hacking

Cyber Arms Control

- The question of how we control, manage, and mitigate the challenges, threats, and dangers posed by “cyber” is perhaps one of the most talked about security problems of our time.
- For sure, there have been attempts to get to grips with the potential hazards posed by hackers to the computer systems, networks and digital data that govern the modern world1, but the cupboard remains bare when it comes to outlining any significant and long-lasting successes in this regard.

Cyber Arms Control

- Part of the reason for this is because the nature of the “cyber” problem still remains to be fully fleshed out and agreed, and it seems very difficult to begin constructing solutions before marking out exactly what it is that we are trying to “control”.
- Thus, it is not simply the case that “cyber” arms control is impossible or that the cyber challenge represents the latest nail in the coffin of the broader international arms control agenda.

1. It will depend upon what we seek to "control" and what we mean by "cyber"

- At the heart of the "cyber arms control" puzzle must be a greater awareness of what we mean by both "cyber" and "arms control".
- "Cyber" as a concept is inherently contested and use of the word often serves to complicate and obfuscate rather than clarify a particular challenge or problem involving computers and networks.
- Likewise, we tend to have a very blinkered understanding of what is meant by "arms control" and what arms control agreements might look like.

1. It will depend upon what we seek to "control" and what we mean by "cyber"

- Taken together, this is not a particularly auspicious starting point for arms control in the digital realm, but it does suggest that clarity in the language we use and the way that we think through the problem is the more sensible and conducive place to begin before we can start designing complex agreements.
- It also produces an important first-order question: what exactly are we trying to "control" and how?

Four Imp. Aspects

- First, are the distinct differences between very low-level activities such as cyber-crime, hacktivism and nuisance–which are probably not best addressed through arms control, and operations that seek to cause damage and disruption, or use "cyber weapons" which might be.
- Second, are the differences between a very narrow conception of the problem focussing purely on Computer Network Attacks against a broader and more inclusive conception involving people, machines and the global digital information environment. Again, narrow definitions seem more suitable for our purpose.

Four Imp. Aspects

- Third, is the distinction between activities that seek to alter the information space (broadly synonymous with Information Warfare/Operations) and those that target information systems directly– realistically it is the latter that we should seek to, and are likely to be able to, control.
- Fourth, is the distinction between the challenges of protecting systems and preventing malicious activities, which may require quite different arms control apparatus.

- 2. “Cyber” arms control will probably be quite different from the nuclear realm
- “In the “cyber realm”... it might not necessarily be at the nation-state or the international level where arms control takes place.”