Cybersecurity

Course Rationale

1.Increased dependence of nations on cyberspace for information, communication economics, entertainment has made it the new global common. It not only presents great opportunities for human development, but it also renders nations extremely vulnerable to cyber exploitation by state as well non-state actors. Adoption of net-centric capabilities by military, civilians and commercial sectors has made the operations of all these entities extremely vulnerable to cyberattacks. The information revolution has transformed the way of thinking, working, acting, transacting, performing and warfighting. Cyberattacks by Russia against Estonia and Georgia and the Israeli and US Stuxnet attack against the command-and-control systems of the Iranian uranium enrichment centrifuges has made the cyber threat, a clear and present danger.

2.Cyberspace is now recognized as the fifth domain of warfare. The anonymity attached with cyber operations and absence of globally accepted treaties or conventions in cyber warfare have resulted in varied definitions of cyber warfare. Every modern nation state is undertaking all measures to defend itself against cyber-attacks and to able to launch a cyber offensive. Cyber surveillance is a norm now and neither foe nor friend is spared. Damaging an adversary’s nuclear facilities by using malware like STUTXNET/FLAME, renders the use of physical armed assaults pointless. No global treaty covers the question of cyber arms control, intricacies associated with a declared or otherwise cyber conflict and its resolution/medication, complexities associated with acts of cyber terrorism by state or non-state entity etc. Legal aspect of cyberattacks are still being discussed at international forums such as the NATO Cooperative Cyber Defense Center for Excellence (CCDOE) Tallin.

3.Pakistan is as vulnerable to cyber threats as any other country; therefore, national policy planners cannot afford to overlook this important dimension of state security.

Educational Objectives

4.The course presents an opportunity for a stringent analysis of prevalent ‘**cyber threat matrix as a not-traditional security issue.’** It also provides tools for preparing policy options for public as well private sector for adoption at all levels.

Input Obtained from Industry/Corporate Sector/Subject Specialists/Academia

5. Report of the webinar organized by the Strategic Vision Institute on 28 January 2021. Pdf available with the author.

International Practice

6. following courses on cybersecurity are being taught in reputed universities:

a. Cybersecurity: The Intersection of Policy with Technology, Harvard Kennedy School, Cybersecurity (Online) | Harvard Kennedy School.

b.MS in Cybersecurity and Public Policy, The Fletcher School, Tufts University.

c.Cybersecurity Policies and Practices in the EU – for non-IT Experts

Proposed Timeframe of Commencement

7.The course is proposed for the Fall 2022 as part of the elective courses to be taught at CIPS

Course Content

8.a.**Course Code**: SS-815

b.**Title**: Cybersecurity

c.**Credit Hours**: 3hrs

d.**Objectives**. To teach students of MS Strategic Studies the basic rules of cybersecurity policy

e.**Outcomes**. The students of this course should be able to:

(1) Plan cybersecurity policies.

(2) Implement cybersecurity policies.

f. **Contents with suggested contact hours:** This will be a 16 classes *3hrs = 48 credit hours course. Following topics will be covered in this module and. The content of the course will be spread along the following topics and issues:

(1) Introduction to cyberspace and cybersecurity

(2) Critical National Infrastructure and homeland security

(3) International norms for cybersecurity

(4) Cyber laws

(5) Cyber International conventions

(6) Cyber CBMs

(7) Cyber diplomacy and deterrence

(8) Cyber emergencies and responses

(9) Cyber terrorism

(10) Cyber weapons

(11) Internet governance

(12) Big data and its protection

(13) Insider threats

(14) United Nations (UN) Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security

g. **Details of lab work, workshops practice (if applicable).** NA

h. **Recommended Reading (including Textbooks and Reference books).**

(1) Alberts, David S., Garstka John J., Stein, Fredrick P. Netcentric Warfare: developing and Leveraging Internet Superiority (CCRP: 2005)

(2) Bartlett, Jamie. *The Dark Net: Inside the Digital Underworld* (Melville House, 2015).

(3) Clarke, Richard A. and Robert E. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (2012).

(4) Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (2015).

(5) Harris, Shane. *@War: The Rise of the Military-Internet Complex* (Eamon Dolan/Mariner Books: 2015).

(6) Krebs, Brian. *Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door Paperback* (Sourcebooks: 2015).

(7) Prevention of Electronic Crime Act (PECA) 2015, http://www.na.gov.pk/uploads/documents/1421399434_340.pdf.

(8) Report of the International Security Cyber Issues, UNIDIR and CSIS, 160816_report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf

(9) Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control* (W.W. Norton and Company: 2016).

(10) Singer, P.W. and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Ecco: 2011).

(11) *Tallinn Manual on the International Law Applicable to Cyber Warfare*, CCDOE, https://ccdcoe.org/research.html.

(12) The Orange Book (Department of Defense Trusted Computer System Evaluation Criteria), http://csrc.nist.gov/publications/history/dod85.pdf.

(13) The Red Book (A Roadmap for Systems Security Research), https://ec.europa.eu/digital-single-market/en/news/red-book-roadmap-systems-security-research.

(14) Yamin, Tughral. *Cyberspace CBMs between Pakistan and India* (NUST, 2014).

(15) Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (2015).