| | |
|---|---|
| COURSE CODE | S6038 |
| COURSE TITLE | **Conflicts in the *Digital* Age:**<br>**Information Operations and Cyber Warfare** |
| ACADEMIC YEAR / TRIMESTER | 2022/23 / T3 |
| LECTURER | Dr Michael Raska |
| EMAIL | ismraska@ntu.edu.sg |
| CLASS DAY / TIME / VENUE | |

## COURSE DESCRIPTION

This course offers an introductory view on the evolving concepts, processes, and debates of information and cyber conflicts whether in political, military, socio-economic, and intelligence domains that are shaping international security. The goal is to provide students with an overall but solid knowledge of cyber and information operations and to encourage them to find their own personal interest in the broad variety of topics these areas offer.

Specifically, the first half of the course is devoted primarily to excavating the historical, theoretical, and conceptual components of cyber and information operations. The second half of the course then focuses on particular case studies of both state and non-state actors – how they conceptualize, plan, integrate, and exploit varying cyber-enabled means to advance their political objectives. The highlight of the course will be the SIMULATION EXERCISE; the "game" will focus on the use of cyber strategic interactions and political decision-making in a crisis situation.

## COURSE OBJECTIVES

This course is aimed to help students:

- Get an overview of the evolving cyber-enabled conflict spectrum shaping international and national security
- Understand key concepts and theories of military cyber and information operations, cyber security debates and hybrid warfare
- Think critically and analytically about the strategic choices and policy options for governments and militaries in dealing with cyber and hybrid conflict challenges
- Assess the possibilities of international cooperation in dealing with cyber problems
- Learn to plan and devise effective responses - cyber-defence strategies

## COURSE OUTLINE

**WEEK 1:** Introduction – Class Requirements, Structure, Format
**WEEK 2:** History of Cyber, Information, and Hybrid Warfare
**WEEK 3:** Strategy and Cyber Power
**WEEK 4:** Cyber Espionage & Advanced Persistent Threats (APTs)
**WEEK 5:** Weaponised Code and the Militarization of Cyber Space: Strategies and Tactics [REACTION ESSAY DUE]
**WEEK 6:** Cyber Crime and Cyber Terrorism
**WEEK 7:** Fighting for Minds: Deception, Disinformation, and Propaganda [OP-ED DUE]
**WEEK 8:** Strategic Information Warfare and Hybrid Conflicts
**WEEK 9:** Preventing & Managing Cyber-Information Conflicts
**WEEK 10:** *Student Presentations [GROUP PROJECT – CYBER DEFENCE STRATEGY DUE]*
**WEEK 11:** *Student Presentations*
**WEEK 12:** CYBER SIMULEX 2023: VIRTUAL SIMULATION GAME
**WEEK 13:** Recap and Final Assignment: *[FINAL POLICY MEMO DUE]*

## COURSE EVALUATION

- Students do not need to possess any advanced technical knowledge. Prior knowledge of the cyber domain is not a prerequisite.

- Students are required to attend all classes; one absence is acceptable without MC.

- The course will be conducted seminar style, with the instructor lecturing initially to set the context and to deal with key terms and ideas, followed by structured and open discussion with a focus on strategy and policy options on the issue.

- There will be “class discussion” questions every week. Students should come into class prepared to develop answers to these questions during discussion. I will call on students in class to share their thoughts.

- It is important to bear in mind that the approach here is twofold: a critical assessment of the concepts and arguments presented in the readings; and a problem-solving concern in which we think about the implications for policy – for national governments, strategy – for military organisations, and international security.

The following scale will be used to issue the final grade in the course:

| | | |
|---|---|---|
| **Reaction Essay** | 20% | Due date: Week 5 |
| **Op-ed** | 10% | Due date: Week 7 |
| **Group Project: Cyber Defence Strategy** | 30% | Due date: Week 10 |
| **Final Assignment: Policy Memo** | 30% | Due date: Week 13 |
| **Active Participation** | 10% | |

**Reaction Essay (or response) Paper: 20%**

Due in Week 5, it should be 1,500 words in length. Week 5 deals with "Weaponised Code and Militarisation of Cyber Space".

Here are some guides on how to write a reaction paper:

- https://www.wikihow.com/Write-a-Reaction-Paper
- http://web.mnstate.edu/robertsb/313/Reaction%20paper%201.pdf
- https://twp.duke.edu/sites/twp.duke.edu/files/file-attachments/response-paper.original.pdf.

Reaction papers are **NOT summaries of the week's readings**. They are intended to get students to react to the main arguments and implications of the readings. Some restatement of the main arguments and recommendations of the readings may be necessary but only so that your own assessment can be clearly stated. The assessment would have two parts. First, do you agree with the key arguments of the readings in terms of the causes of the problem in Week 5? If so, why? If not, why? Secondly, what are the implications for strategy and policy? If you were a defence policy maker, what lessons would you take away from the readings (including negative lessons i.e. what not to do)?

**Op-ed: 10%**

Writing an op-ed is a skill all students at a professional school should learn. It is a highly visible form of communicating, can have a very large audience, and can be influential with the reading public as well as government officials. Op-ed lengths vary from 650-700 words long to 1000-1200 words. For this class, 1000 words is a good length. You must write exactly 1000 words, as newspapers are quite precise on length requirements. The assignment is due in **Week 7.**

**See:** How to write an op-ed by a *New York Times* writer:
https://www.nytimes.com/2017/08/25/opinion/tips-for-aspiring-op-ed-writers.html.

**See:** Here is another from Harvard University: https://journalistsresource.org/tip-sheets/writing/how-to-write-an-op-ed-or-column.

**Group Project (3 students per group) : Cyber Defence Strategy: 30 %**

As cyber challenges are growing rapidly, policy-makers must tackle emerging challenges, but have divergent views on how to prioritize the risks and responsibilities. Many countries cybersecurity strategy are becoming outdated. In this assignment, your task is devise a national cyber defence strategy for a select state – corporation – or international organization, including action plans to implement and maintain such a strategy, keeping it relevant. That includes creating crisis resilience at different levels of society.

The strategy should be a realistic policy document, which integrate key elements of formal paper assignment such as citation standard (both Harvard and Chicago Manual of Style are fine), footnotes, etc. The documents should be about 4 - 5000 words in length, properly referenced and submitted to the lecturer by **Week 10** or earlier. Late submissions will be penalized. Students should confirm their intended project by Week 3-4.

**See: CCDCOE, "Guide to Developing a National Cybersecurity Strategy - Strategic Engagement in Cybersecurity 2018,"** Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

**See: ITU Repository of National Cybersecurity Strategies:** https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

**Final Assignment: Policy Memo: 30 %**

The final assignment will be a policy memo, about 2,000 words in length. A policy memo is a short document with a clear statement of the policy challenge, the background and context to the challenge, the options available and the pros and cons of each option, and finally a recommendation for action. **Policy Memo can be based on any topic covered in the course.**

See Example: https://www.csis.org/analysis/options-hong-kong-suggested-nsc-memo

Please use its format in doing your policy memo. The CSIS memo is more than 2000 words long, but please restrict yourself to 2000 words for the final assignment.

**Writing assessments**: In all writing assessments, students will be judged on organisation, clarity of expression, and logical development of the argument(s). **There will be penalties for late submission of the reaction paper, the op-ed, or final project.**

**Active Class Participation: 10 %**

Active class participation helps students to put forward their arguments and critically engage the readings. It also gives them an opportunity to appreciate various points of view on a subject. Active participation means informed participation with a view to enhancing discussions and learning. Students will be graded on the *quality and quantity* of their interventions in class. *You will be graded for participation over the course of the entire semester*.

## PLAGIARISM

Nanyang Technological University (NTU) takes a tough stance on plagiarism and none will be tolerated. The penalties for academic dishonesty reflect NTU's strong commitment to academic integrity and include: expulsion, suspension, zero mark/fail grade, a requirement to resubmit the assignment/dissertation or marking down. Please ensure you understand and abide by the NTU Academic Integrity Policy. In taking this course, students are understood to be fully cognizant of all relevant university guidelines and regulations. For further guidance please refer to the full policy online: http://www.ntu.edu.sg/ai/Pages/index.aspx

## READINGS

The readings have been listed in order of the professor's ranking as to importance. At the same time, the reading list is only a good starting point for considering the issues to be discussed. As in all subjects, the list of material is endless; the mark of a good scholar is to first find material that is relevant to their individual studies, and second to be able to analyze and synthesize the material into coherent arguments. As such, students are expected to exercise their initiative in reading within and beyond this list. Indeed, the ability to source for data independently will constitute a key element in the student's assessment.

## COURSE STRUCTURE

### WEEK 1: Course Introduction (ONLINE)

- **Course Overview, Requirements, Structure, Format**

### WEEK 2: History of Cyber, Information, and Hybrid Warfare

- *** Christopher Whyte and Brian Mazanec,** *Understanding Cyber Warfare: Politics, Policy and Strategy*, Chapter 6 – "A Brief History of Major Cyber Conflict Episodes." (London: Routledge 2018).

- *** Michael Raska,** "The sixth RMA wave: Disruption in Military Affairs?" *Journal of Strategic Studies*, Vol 44, No. 4 (2021). Available at: https://doi.org/10.1080/01402390.2020.1848818

- ***John Arquilla and David Ronfeldt.** "The Advent of Netwar Revisited." In : *Networks and Netwars: The Future of Terror, Crime, and Militancy*. (Santa Monica: RAND, 2001). Available at: http://www.rand.org/pubs/monograph_reports/MR1382.html

- *** Peter W. Singer and Allan Friedman** (2014) *Cybersecurity and Cyberwar. What Everyone Needs to Know* (Oxford University Press: Oxford), pp. 13–66.

- **Nilsson, Niklas, Mikael Weissmann, Björn Palmertz, Per Thunholm, and Henrik Häggström.** "Security challenges in the grey zone: Hybrid threats and hybrid warfare." In: Hybrid Warfare: Security and Asymmetric Conflict in International Relations. By Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm . London: I.B. Tauris, 2021. 1–18. Bloomsbury Collections. Web. 23 Apr. 2021. Available at: http://dx.doi.org/10.5040/9781788317795.0005

- **Ben-Israel Isaac and Tabansky Lior,** "An Interdisciplinary Look at Security Challenges in the Information Age", *Military and Strategic Affairs*, Vol. 3 No 3, December 2011. Available at: http://www.inss.org.il/uploadimages/Import/(FILE)1333532835.pdf

- **NATO Science & Technology Organization**, "Science & Technology Trends 2020-2040," Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

- **Channel News Asia (2020)**: "Secret Wars" - The Cybersecurity Dilemma https://www.channelnewsasia.com/news/video-on-demand/secret-wars/the-cybersecurity-dilemma-12560614

*Class Discussion:*

- How do cyber, information, and hybrid warfare differ from traditional threats and warfare?
- How revolutionary is cyberspace?
- What are the effects of cyber weapons on international stability?

## WEEK 3: Strategy and Cyber Power in the Automation Age

*__Required reading__

- *** Jon Lindsay,** "Restrained by Design: The Political Economy of Cyber Security," *Digital Policy, Regulation and Governance*, Vol. 19 No. 6, pp. 493-514. Available at: https://doi.org/10.1108/DPRG-05-2017-0023

- *** Marcus Willett,** "Cyber Instruments and International Security," *IISS*, 12 March 2019, https://www.iiss.org/blogs/analysis/2019/03/cyber-instruments-and-international-security

- *** Lucas Kello,** "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* Fall 2013. Available at: http://www.mitpressjournals.org/doi/pdfplus/10.1162/ISEC_a_00138

- *** John Sheldon,** "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly*, Summer 2011, Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a544498.pdf

- *** Colin S. Gray,** "Making Strategic Sense of Cyber Power: Why the Sky is not Falling," Strategic Studies Institute, 2013, 1-54. Available at: https://publications.armywarcollege.edu/pubs/2219.pdf

- **IISS,** "Cyber Capabilities and National Power: A Net Assessment." *IISS Report* (2021). p.1-14. Available at: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

- **Joseph Nye,** "Cyber Power" Report published by the Belfer Center for Science and International Affairs (2010); Available at: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

- **Michael C. Horowitz, Gregory C. Allen, Elsa B. Kania, and Paul Scharre**, "Strategic Competition in an Era of Artificial Intelligence," Center for a New American Security Report series on Artificial Intelligence and International Security, July 2018, Available at: https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence

- **Clark, Justin, Robert Faris, Ryan Morrison-Westphal, Helmi Noman, Casey Tilton, Jonathan Zittrain**. "The Shifting Landscape of Global Internet Censorship." Berkman Klein Center for Internet & Society, Harvard University. June 2017. Available at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:33084425

*Class Discussion:*

- What is cyber power?
  Why is cyber power is inherently restrained by cyber 'entanglement'?
- What are strategic implications of cyber revolution?

Does cyber power require a revolution in how scholars and policymakers think about the use of force and conflict?

## WEEK 4: Cyber Espionage and Advanced Persistent Threats

- * **Devanny, Joe, Ciaran Martin, and Tim Stevens**. "On the Strategic Consequences of Digital Espionage." *Journal of Cyber Policy* (2021): 1-22. https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.2000628

- *** Michael Warner**, "Intelligence in Cyber - and Cyber in Intelligence," In George Perkovich and Ariel E. Levite (eds.) *Understanding Cyber Conflict: Fourteen Analogies* (Washington D.C.: Georgetown University Press, 2017). Available at: http://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_Ch1.pdf

- *** Jon Lindsay and Tai Ming Cheung,** “From Exploitation to Innovation: Acquisition, Absorption, and Application,” Chapter 3. In Jon Lindsay, Tai Ming Cheung, and Derek Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York, NY: Oxford University Press, 2015). Available at NTULearn.

- **FireEye**, “Advanced Persistent Threat Groups - Who's Who of Cyber Threat Actors,” Available at: https://www.fireeye.com/current-threats/apt-groups.html
  Example: https://content.fireeye.com/apt-41/rpt-apt41/

*Class Discussion:*

- How does cyber espionage affect international security?
- Governments have been quick to adopt cyber means as a tool for intelligence gathering, attracted both by the large amounts of sensitive information stored and transmitted on computer networks as well as the difficulties of sure attribution of cyber intrusions. Should governments increase their resource allocation to cyber espionage?

## WEEK 5: Cyber Operations: Weaponized Code and Militarization of Cyberspace

**REACTION-ESSAY ASSIGNMENT DUE**

- *** Thomas Rid**, “Cyber War Will Not Take Place.” *Journal of Strategic Studies* Vol. 35 No.1 (2011): 5-32. https://doi.org/10.1080/01402390.2011.608939

- *** Tianjiao Jiang**, “From Offense Dominance to Deterrence: China’s Evolving Strategic Thinking on Cyberwar,” *Chinese Journal of International Review*, vol. 1, no. 2 (2019). Available at: https://www.worldscientific.com/doi/pdf/10.1142/S2630531319500021

- *** Adam Segal,** “U.S. Offensive Cyber Operations in a China-U. S. Military Confrontation.” In: Herbert Lin and Amy Zegart (eds), *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington D.C., Brookings Institution Press, 2018).

- *** Andreas Krieg & Jean-Marc Rickli**, “Surrogate Warfare: The Art of War in the 21st Century?” *Defence Studies*, 18:2, 113-130. https://doi.org/10.1080/14702436.2018.1429218

- **Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata.** “Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War.” *Security*

*Dialogue* 43, no. 3 (2012): 3–24  Available at: https://www.jstor.org/stable/26301960

- **McGuiness, Damien**. “How a Cyber Attack Transformed Estonia.” BBC, 27th April 2017. https://www.bbc.com/news/39655415

- **Thomas Rid & Ben Buchanan**, “Attributing Cyber Attacks.” *Journal of Strategic Studies*, Vol. 38 No 1-2 (2015), 4-37, https://doi.org/10.1080/01402390.2014.977382

- **Christopher Bronk and Eneken Tikk-Ringas**, “The Cyber Attack on Saudi Aramco,” *Survival,* vol.55, no.2, 2013. https://doi.org/10.1080/00396338.2013.784468

- **Demchak, Chris C., and Peter Dombrowski**. “Cyber Westphalia: Asserting State Prerogatives in Cyberspace.” *Georgetown Journal of International Affairs*, no. 20 (2014): 29–38. https://www.jstor.org/stable/43134320

- **UNIDIR,** "The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations," UNIDIR Report 2017. https://www.unidir.org/publication/weaponization-increasingly-autonomous-technologies-autonomous-weapon-systems-and-cyber

- **David Sanger,** *Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power* (New York: Crown, 2012): Lecture:  https://youtu.be/TsimILLpu0M

- **Michael Raska,** “North Korea’s Cyber Strategies: Continuity and Change.” *SIRIUS – Journal of Strategic Analysis*. Vol 4. No. 2 (2020), 144-158.

*Class Discussion:*

- What is cyber war? Is it really coming? Does it even exist?
- Can we effectively deter cyber-attacks?
- What are strategic dilemmas or trade-offs of using military cyber operations?

## WEEK 6: Cybercrime and Cyberterrorism

- *** FireEye Mandiant**, “M-Trends 2021 Report,” Available at: \ https://www.arrow.com/ecs-media/16352/fireeye-rpt-mtrends-2021.pdf

- *__Trend Micro__, “Attacks from All Angles - 2021 Mid-year CyberSecurity Report.” Available at: https://documents.trendmicro.com/assets/rpt/rpt-attacks-from-all-angles.pdf

- *** Kristin Finklea,** “Dark Web,” A Congressional Research Service Report (R44101), March 10, 2017. Available at: https://fas.org/sgp/crs/misc/R44101.pdf

- **UNODC**, "Darknet Cybercrime Threats to Southeast Asia 2020" Available at: https://www.unodc.org/documents/southeastasiaandpacific/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf

- **Vincenzo Ciancaglini (et.al.),** “Below the Surface: Exploring the Deep Web,” A TrendLabsSM Research Paper, Available at: https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf

- **Martin Rudner,** “Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge,” *International Journal of Intelligence and CounterIntelligence*, 26:3, 453-481.

- **Michael Kenney,** “Cyber-Terrorism in a Post-Stuxnet World,” *ORBIS*, vol. 59, no. 1 (Winter 2015).

*Class Discussion:*

- What is the difference between terrorism and cyber terrorism?
- How can modern terrorist groups use cyber means to their advantage?

## WEEK 7: Fighting for Minds: Deception, Disinformation, and Propaganda

**OP-ED ASSIGNMENT DUE**

- *** Alice Marwick and Rebecca Lewis,** “Media Manipulation and Disinformation Online,” *Data & Society Research Institute*, Available at: https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf

- ***Adrienne LaFrance**, “The Prophecies of Q,” *The Atlantic*, June 2020. https://www.theatlantic.com/magazine/archive/2020/06/qanon-nothing-can-stop-what-is-coming/610567/

- ***Todd C. Helmus et. al.** *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: RAND Corp., 2018). Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf

- **Soroush Vosoughi, Deb Roy, Sinan Aral,** “The Spread of True and False News Online" *Science*, Vol. 359, Issue 6380, 09 Mar 2018. pp. 1146-1151. https://www.science.org/doi/10.1126/science.aap9559

*Class Discussion:*

- What is the power of online propaganda?
- What capabilities are needed to identify and counter information influence activities?
- What role and responsibilities have Big Tech companies in tacking disinformation?

## WEEK 8: Strategic Information Warfare and Hybrid Conflicts

- *** Dima Adamsky,** “Cross-Domain Coercion: The Current Russian Art of Strategy,” *Proliferation Papers*, vol. 54, IFRI Security Studies Center, 2015, Available at: http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf

- *** Weissmann, M.** (2021). “Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone.” In M. Weissmann, N. Nilsson, B. Palmertz & P. Thunholm (Authors), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (pp. 61–82). London: I.B. Tauris. http://dx.doi.org/10.5040/9781788317795.0011

- *** Lachlan Brumley, Carlo Kopp, Kevin Korb,** “Cutting Through the Tangled Web: An Information-Theoretic Perspective on Information Warfare.” *Air Power Australia Analysis* 2012. Available at: http://www.ausairpower.net/APA-2012-02.html

- *** Marvin Kalb,** “The Israeli—Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict.” *The Harvard International Journal of Press/Politics* No. 12 (2007): 43-66. Available at: https://doi.org/10.1177%2F1081180X07303934

- **G.J. David and T.R. McKeldin** (eds.) (2009) *Ideas as Weapons: Influence and Perception in Modern Warfare* (Washington D.C.: Potomac Books): Short Essays 2.

*Class Discussion:*

- What is the difference between hybrid and grey zone operations?
- Are Western societies less resilient to hybrid warfare threats?

## WEEK 9: Preventing and Managing Cyber-Information Conflicts

- * **Joseph Nye,** "The End of Cyber-anarchy? How to Build a New Digital Order," *Foreign Affairs,* vol. 101, no. 1, Jan/Feb 2022, pp. 32-42 https://www.foreignaffairs.com/articles/world/2021-12-14/end-cyber-anarchy

- *** Rogier Creemers,** "China's Approach to Cyber Sovereignty," Konrad Adenauer Stiftung, 2020, Available at: https://www.kas.de/en/single-title/-/content/china-s-approach-to-cyber-sovereignty

- *** Claessen, Eva**. "Reshaping the Internet – The Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU." *Journal of Cyber Policy* 5, no. 1 (2020): pp. 140–157. Available at: https://doi.org/10.1080/23738871.2020.1728356

- *** Netherlands Presidency of the Council of the EU.** "Non-Paper: Developing a Joint EU Diplomatic Response against Coercive Cyber Operations," 5797/6/16REV6. 19th May 2016. http://statewatch.org/news/2016/jul/eu-council-diplomatic-response-cyber-ops-5797-6-16.pdf

- **SCHMITT, Michael N.** *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press. 2017. Chapter 1 – Sovereignty. Pp.11-29.

- **Vendil Pallin, Carolina and Mattias Hjelm**. "Moscow's Digital Offensive – Building Sovereignty in Cyberspace." Swedish Defence Research Agency, 2021. Available at: https://www.foi.se/rapportsammanfattning?reportNo=FOI%20Memo%207521

- **Dewar, Robert,** "Active Cyber Defence", *CSS Cyber Defence Trend Analysis 1*, ETH Zurich, 2017, Available at: https://doi.org/10.3929/ethz-b-000169631

*Class Discussion:*

- Two broad foreign policy approaches to the Internet have emerged: one advocates a free, open, global Internet and a multistakeholder model of global governance involving states and private actors, while the other supports limiting the flow of certain information online and a state-centric, multilateral model of governance. What motivates each of t ese approaches?
- Can cyberattack escalation be prevented, controlled, or managed?
- How will emerging technologies shape the future of war and conflict?

## WEEK 10: Student Presentations + GROUP PROJECT DUE

As cyber challenges are growing rapidly, policy-makers must tackle emerging challenges, but have divergent views on how to prioritize the risks and responsibilities. Many countries cybersecurity strategy are becoming outdated. In this assignment, your task is devise a national cyber security strategy for a select state, including action plans to implement and maintain such a strategy, keeping it relevant. That includes creating crisis resilience at different levels of society.

The strategy should be a realistic policy document, which integrate key elements of formal paper assignment such as citation standard (both Harvard and Chicago Manual of Style are fine), footnotes, etc. The documents should be about 5000-7000 words in length, properly referenced and submitted to the lecturer by **Week 10** or earlier. Late submissions will be penalized. Students should confirm their intended project by Week 3-4.

**See: CCDCOE, "Guide to Developing a National Cybersecurity Strategy - Strategic Engagement in Cybersecurity 2018,"** Available at:
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf
**See: ITU Repository of National Cybersecurity Strategies:**
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

## WEEK 11: Student Presentations – Cyber Defence Strategies

Group presentations

## WEEK 12: Cyber SIMULEX 2023: Virtual Simulation Game

Building upon both theoretical and empirical foundations of the course, the final simulation exercise will emulate a specific cyber crisis scenario. Guidelines and instructions will be distributed two weeks prior to the game in order to ensure that the simulation accurately reflects, to the extent possible, a real scenario. The single most important factor is to think, reflect, act, and respond in a way the particular actor is likely to act. In other words, it's not your views that are important but those of the governments, institutions, or individuals you are trying to emulate. Members of the individual teams should act as a *team* and remember to accurately reflect current capabilities, data, policies, strategies, etc.

One of the most important aspects of a game is to provide a thorough review of the game in order to provide an objective assessment of the strengths and weaknesses of the game and the teams. Each team's monitor will provide a quick review of the key decisions made by the teams while the team leaders will provide each team's perception of the scenario, the forces which compelled them to act, and their thinking process throughout the different phases of the game.

The Control Team will assess the following aspects of the game in its final post-game report:

"TMIs": Triggers, Magnitude, Impact
"3R's": Response, Recovery, Reconstitution

B. Capacity and Capabilities
C. Strategic and Tactical Lessons
D. Guidelines for future crisis and consequence management

## WEEK 13: Recap & Final Assignment – Policy Memo

The final assignment will be a policy memo, about 2,000 words in length.  A policy memo is a short document with a clear statement of the policy challenge, the background and context to the challenge, the options available and the pros and cons of each option, and finally a recommendation for action.  **Policy Memo can be based on any topic covered in the course.**

See Example: https://www.csis.org/analysis/options-hong-kong-suggested-nsc-memo
Please use its format in doing your policy memo. The CSIS memo is more than 2000 words long, but please restrict yourself to 2000 words for the final assignment.