# Cyberspace, Terrorism and Counterterrorism

**Dr. Myriam Feinberg**

**Course Number:** 702.2980
**Class Time**: Monday 12:00-15:00
**Class Location: TBA**
**E-Mail:** myriam.ap@gmail.com

## Module description:

This module examines the concepts of cyberterrorism and counterterrorism and provides both a general introduction to cybersecurity and an analysis of practical applications of the use of the Internet both for terrorism purposes and for countering terrorism.
It addresses such timely issues as state to state cyber-attacks, and whether this could amount to an armed attack under international law raising issues of self-defense; cyber attacks by non-state actors; the role of non-state actors, such as hacktivists, in both contributing to and reducing the terrorist threat; the issue of incitement to terrorism and recruitment, and the necessary balance with freedom of speech; as well as the issue of surveillance and the delicate balance between security needs and privacy.

Recent examples, which will be covered in the module include the decision by the President of the United States to impose sanctions against Russia for its interference in the U.S. through 'significant malicious cyber-enabled activities'; as well as the use of social media by terrorists.

The module will be taught with reference to primary sources and Internet resources, such as presidential executive orders imposing sanctions against cyber attacks or dedicated websites for flagging illegal content on social media, as well as to secondary sources from legal and security experts.

## Course Requirements:

- Weekly reading list and active class participation
- 5 one-page reaction papers (choice of the student) over the course of the module
- Mid-term exam
- Final assignment

## Final Grade:

- Reaction papers (1 page each) and participation: 35%
- Mid-term exam (in class): 15%
- Final assignment (at home essay): 50%

## Course Outline and Reading List (may be subject to changes throughout the semester)

**General information**
How to write a reaction paper? (available on Moodle)

**Week 1 – Introduction**

**Week 2 – Terrorism – Definitions and trends Reading**

- Gilbert Ramsay (2015) 'Why terrorism can, but should not be defined', 8 *Critical Studies on Terrorism*, 2, 211-228
- Understanding Terrorism Today and Tomorrow, July 2015, Volume 8, Issue 7, General Joseph L. Votel

**Week 3 – Counterterrorism issues**

- ISIS in the United States, Aaron Jackson, Just Security
- Terrorism and counterterrorism: an overview, Todd Sandler, Oxford Economic Papers, Volume 67, Issue 1, 1 January 2015, Pages 1–20,

**Week 4 – Cyberspace – definition, issues**
**Reading**

- Gabriel Weimann (2016), 'Going Dark: Terrorism on the Dark Web', 39 *Studies in Conflict & Terrorism* 3.
- Michael Chertoff, A Public Policy Perspective of the Dark Web, Chatham House

**Week 5 – Cyber terrorism – actors**
**Reading**

- Grey Hat, Reese Wiedman, NYMag, 2018
- Keiran Hardy, George Williams (2014), 'Terrorist, Traitor, or Whistleblower - Offences and Protections in Australia for Disclosing National Security Information'37 *University of New South Wales Law Journal* 784
- The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain, April 2018, Volume 11, Issue 4, Nafees Hamid

**Week 6 – Regulatory framework against cyber terrorism**
**Reading**

- David Fidler (2016), 'Cyberspace, terrorism and International law', 21 *Journal of Conflict & Security Law* 3, 475–493
- Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace, August 2012, Volume 5, Issue 8, Jonalan Brickey

**Week 7 – Mid-term exam (in class) and Guest lecture**

**Week 8 – Cyber crime and terrorism**
**Reading**

- The Cybercoaching of Terrorists: Cause for Alarm? October 2017, Volume 10, Issue 9, John Mueller
- Financing Terror Bit by Bit, October 2014, Volume 7, Issue 10, Aaron Brantly

**Week 9 – Cyber attacks**
**Reading**

- Blog post about Tallinn manual and Tallinn Manual 2.0: https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/
- Nicholas Tsagourias (2012), 'Cyber attacks, self-defence and the problem of attribution', 17 *Journal of Conflict and Security Law* 2, 229–244

**Week 10 – Communications and privacy, espionage**
**Reading**

- Banks, William, Cyber Espionage, Surveillance, and International Law: Finding Common Ground (October 17, 2014)
- How Terrorists Use Encryption, June 2016, Volume 9, Issue 6 Robert Graham

**Week 11 – online incitement**
**Reading**

- Yael Ronen (2010) 'Incitement to Terrorist Acts Under International Law', 23 *Leiden Journal of International Law* 3.
- Ezekiel Rediker (2015) 'The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union', 36 *Michigan Journal of International Law* Volume 2.

**Week 12 – documentary**