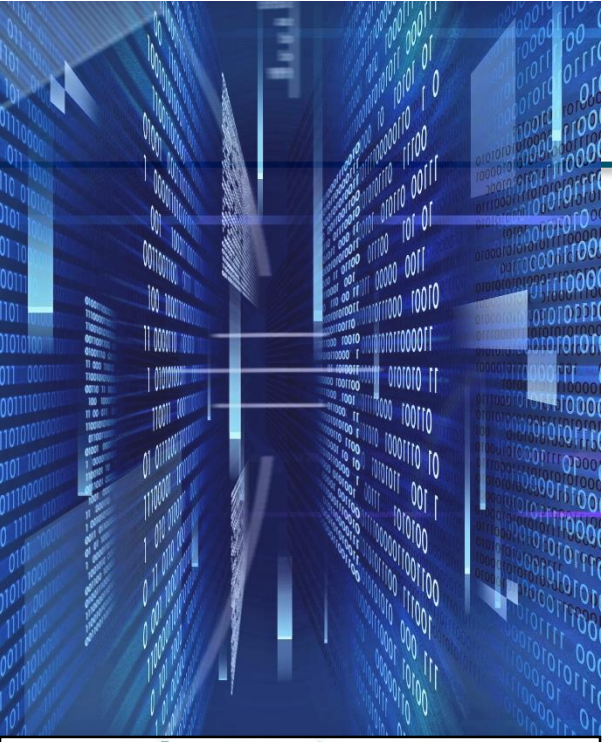

cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

Cybersecurity Southampton

Cyber Security Research Group

blog | twitter

UNIVERSITY OF Southampton

COMP6224 2019-20
Foundations of Cyber Security

Cyberwarfare and Hacktivism

Week 9 – Friday 29th November 2019

Dr Leonardo Aniello

l.aniello@soton.ac.uk

Link with previous lectures

UNIVERSITY OF Southampton

Cyber Security

- Cyber Essentials
- Advanced Cyber Defences
- Access Control
- Confidential/anonymous data/communication
- Authentication (include passwords)
- Cryptography

Cyber Space

- Applications
- Data at rest
- Data in transit
- Machines
- Network

Cyber Attacks

- Social Engineering
- Web defacements
- Influence campaigns
- DDoS
- Data breaches
- Ransomware
- Money theft
- Pervasive Passive Monitoring
- Cyber Attack Life Cycle

Cyber Actors

Multi-disciplinary Aspects

- Hacktivism
- Cyberwarfare
- Law

Learning Outcomes

At the end of this lecture you should be able to

- LO1 Discuss the differences between cyberwar and conventional warfare
- LO2 Describe why cyberwar is attractive for Nation States
- LO3 Discuss the ethics, culture and motivations of Hacktivists
- LO4 Describe the main features of Hacktivist groups

Outline

- Cyberwarfare
  - ➢**What is Cyberwarfare?**
  - Cyberwarfare vs conventional Warfare
  - Cyberwar attractiveness
- Hacktivism
  - What is Hacktivism?
  - Ethics and culture of Hacktivists
  - Hacktivist Groups
    - Anonymous
    - WikiLeaks

What is Cyberwarfare?

Cyberwarfare refers to
the common activities and characteristics of types of war
that are carried out through the cyber space

The Cyber Attack on Estonia April-May 2007

- Estonia at the forefront of innovation in cyber technology
  - Great growth and development
  - Cyberspace integral part of most activities

- 26th April 2007: relocation of the monument commemorating the Soviet armed forces' liberation of Estonia from the Nazi

The Cyber Attack on Estonia April-May 2007

- 27th April 2007: a series of cyber attacks began
  - DDoS attacks
  - Ministries of Foreign Affairs' and Justice' websites shut down
  - Prime Minister's Party's website defaced
  - Botnets began attacking private sites and servers, many banks were shutdown, great monetary costs, affected also international banking
  - National emergency toll-free phone number 112 disabled
- Estonian Government blamed the Kremlin, but Moscow denied any involvement in the attacks

What is Cyberwarfare?

- The battlefield includes the cyberspace
  - Greater efficiency, better services but increased vulnerability
  - Network convergence: All communications over a common network
  - Channel consolidation: Concentration of data on a few providers
  - Networked forces: Military innovation enabled by cyber technologies
- Same objectives as conventional warfare
  - Espionage
  - Sabotage
  - Propaganda

Outline

- Cyberwarfare
  - What is Cyberwarfare?
  - ➢ **Cyberwarfare vs conventional Warfare**
  - Cyberwar attractiveness
- Hacktivism
  - What is Hacktivism?
  - Ethics and culture of Hacktivists
  - Hacktivist Groups
    - Anonymous
    - WikiLeaks

Cyberwarfare vs conventional Warfare

- Can cyberwar be considered as a conventional war?
- A conventional war is a state of conflict between states, characterized by violence
- To be considered as “war”, it should cause physical damage or destruction
  - It would have to “proximately result in death, injury or significant destruction” [Koh speech 2011]
  - e.g., a plane dropping bombs is “war”, a plane dropping leaf-lets, not so much

Cyberwarfare vs conventional Warfare

- During cyber attacks to Estonia
  - Estonia demanded NATO intervention
  - NATO disagreed: no casualties, no property damaged

- The way to determine when a cyberattack constitutes the kind of “use of force” that legally justifies war is to weigh its effects

- Severity of the attack is not the only thing
  - Any action that could ultimately spark a chain of events that cause the same death and destruction as traditional war

Can cyberwar be considered as a conventional war?

- War is the **use of force** to cause damage, destruction or casualties for political effect by states or groups
  - Grey area: disruption of data and services **below the level of use of force**
  - The threshold for regarding a cyber incident as the use of force is the most important **ambiguity** in cyberwar

- The **right of self-defence** is triggered by the use of force
  - Only in case of large scale cyber attacks on critical infrastructures with effects comparable to those of an armed attack
    - Significant physical damage
    - Casualties

Cyberwarfare vs conventional Warfare

UNIVERSITY OF Southampton

Can cyberwar be considered as a conventional war?

- There is consensus based on international practice that the following are not acts of war and do not justify the use of force in response
  - Propaganda
  - Harassment
  - Hacktivism
  - Crime
- What about these?
  - Intelligence collection
  - Cyber reconnaissance
- Nondestructive cyber attacks used for cyber espionage may violate the domestic law of the victim nation-state but are not contrary to international law
- Political decision: “The answer to whether a particular attack is an act of war comes down to this: is it in your interest to declare it so?” [Libicki 2009]

Outline

- Cyberwarfare
  - What is Cyberwarfare?
  - Cyberwarfare vs conventional Warfare
  - ➢**Cyberwar attractiveness**
- Hacktivism
  - What is Hacktivism?
  - Ethics and culture of Hacktivists
  - Hacktivist Groups
    - Anonymous
    - WikiLeaks

Cyberwar attractiveness

- Cost effectiveness
  - No need for large numbers of troops and weapons
  - With a computer and Internet, anyone can engage in cyberwar
  - Tools for attack are cheap and openly available on the Internet
- No casualties
- Disrupt the adversary rather than destroy his forces
- Speed of light (almost)
- Hard to detect and neutralize for the victim
- Exploitable vulnerabilities increase with technological evolution

Cyberwar attractiveness

- Anonymity
  - Operate behind false IP addresses, foreign servers and aliases
  - Hard/nearly impossible to trace cyber attack origin
- Attribution is nearly impossible!!
  - Plausible deniability: the attacker can always claim that his computer had been hacked and used in someone else's operation
- Cyber Deterrence
  - Without attribution, deterrence is pointless
  - If retaliation cannot hit the attacker, he will not be deterred
  - Retaliation against the wrong actor is unjust and a crime of war

Outline

- Cyberwarfare
  - What is Cyberwarfare?
  - Cyberwarfare vs conventional Warfare
  - Cyberwar attractiveness
- Hacktivism
  - ➢**What is Hacktivism?**
  - Ethics and culture of Hacktivists
  - Hacktivist Groups
    - Anonymous
    - WikiLeaks

Who are the hacktivists?

- Politically motivated hackers
  - Driven by pursuit of social change
  - Do not seek profit or intellectual pursuit
- Relatively new, but already well-established, form of civic participation

- "Hacktivism is likely to continue to gain attention and will evolve in response to changing global economic and political conditions" [Wray 1998]

From Hacking to Hacktivism

- Hacker Ethics [Levy 1984]
  1. Everyone should have unlimited and unrestricted access to computers
  2. Information wants to be free and, therefore, must be free
  3. One should mistrust any type of authority, and promote decentralization
  4. Hackers are to be judged by their technical abilities, instead of “bogus criteria, such as degrees, age, race, or position”
  5. Hackers’ activities on computers should be considered acts of art and beauty
  6. Computers are thought of as positive phenomenon, which can change one’s life for the better

From Hacking to Hacktivism

- Hacktivists share many principles of hacker ethic
  - Libertarian and anarchist in nature
  - Conceptualised as opponents of the power elite, that use technology to promote their own agendas
- Portrayed by the state and the media as villains and threats to society
  - Equated with cyber terrorism
  - But hacktivists openly condemn cyber terrorism
  - Civil disobedience acts rather than terrorist acts

Outline

- Cyberwarfare
  - What is Cyberwarfare?
  - Cyberwarfare vs conventional Warfare
  - Cyberwar attractiveness
- Hacktivism
  - What is Hacktivism?
  - ➢**Ethics and culture of Hacktivists**
  - Hacktivist Groups
    - Anonymous
    - WikiLeaks

Hacktivist Ethics

- Act of civil disobedience
  - No damage to people or property
  - Non-violent
  - Not for personal profit
  - Driven by strong ethical motivation
  - Will to take personal responsibility for his/her actions
- Hacktivism is different from cyber terrorism
  - Both use technology as a tool
  - Cyber terrorists use violent methods, aim at destruction
  - Hacktivists do not use violent methods, aim at disruption

Hacktivist Culture

- Conspiracy theorising
- Obsession with privacy and secrecy
- Membership fluidity
- Anarchic heritage and anti-capitalist sentiment
- Culture of humour and creativity

Outline

- Cyberwarfare
  - What is Cyberwarfare?
  - Cyberwarfare vs conventional Warfare
  - Cyberwar attractiveness
- Hacktivism
  - What is Hacktivism?
  - Ethics and culture of Hacktivists
  - Hacktivist Groups
    - **Anonymous**
    - WikiLeaks

Anonymous

- Collective, loosely networked movement
  - Anonymous members are known as Anons
  - Guy Fawkes masks as a disguise

- Originated on the message board 4chan.org in 2003
- Began with primarily prankster intentions, later evolved into a more politically-oriented organization

Anonymous

- Pluralistic movement, with complementary views and ideologies [Fuchs 2013]
- Key points [Wong & Brown 2013]
  - Anti-censorship and freedom of speech
  - Privacy
  - Internet security
- Core principles
  - The media should not be attacked
  - Critical infrastructure should not be attacked
  - One should work for justice and freedom

Membership and Governance

- "Anonymous is everyone.
  Anonymous is no one.
  Anonymous exists as an idea"
- All-inclusive: anyone can join or leave the group at any time
- Claims to not have any leadership and/or hierarchy
  - Great adaptability and resilience
  - There are core activists within Anonymous "with specific technical skills, media skills, and organizational skills who carry out the core of hacking activities" [Fuchs 2013]
- Relies on a critical mass
  - For DDoS attacks, through software such as LOIC and HOIC
- Community-based communications
  - IRCs, message boards, file-sharing

Notable operations

- 2008 Project Chanology – against the Church of Scientology
- 2010 Operation Payback – against Aiplex Software, which launched DDoS attacks on websites sharing copyrighted resources (e.g. The Pirate Bay)
  - Then also targeted RIAA and MPAA
- 2010 Operation Avenge Assange
  - Against PayPal, PostFinance, EveryDNS
- 2011 Operation Darknet: against websites hosting child pornography
- 2013 Massive cyber-assault against Israel for its actions in Gaza
- …
- 2017 Operation Darknet Relaunch: against Tor-based websites hosting child pornography

Outline

- Cyberwarfare
  - What is Cyberwarfare?
  - Cyberwarfare vs conventional Warfare
  - Cyberwar attractiveness
- Hacktivism
  - What is Hacktivism?
  - Ethics and culture of Hacktivists
  - Hacktivist Groups
    - Anonymous
    - **WikiLeaks**

WikiLeaks

- “multi-national media organization and associated library”
- Non-profit organization, publishes censored or restricted documents
  - More than 10 million documents in 10 years
- Initiated in 2006 in Iceland, Julian Assange its founder
  - wikileaks.org domain
- Purpose
  - Bring important information to the public
  - Allow journalists/whistleblowers to disclose sensitive/classified documents without being prosecuted

WikiLeaks

- Bulletproof hosting
  - Mainly hosted by Bahnhof ISP in Sweden
  - Other servers spread around the world
  - In nations offering legal protection to disclosure
- Some leaks
  - Intelligence (e.g. Vault 7 & 8)
  - Global Economy (e.g. Trade in Services Agreement)
  - International Politics (e.g. Macron Campaign Emails)
  - Corporations (e.g. Hacking Team)
  - War & Military (e.g. Guantánamo Files)

Cyberwarfare and Hacktivism – Recap

- Cyberwarfare
  - What is Cyberwarfare?
  - Cyberwarfare vs conventional Warfare
  - Cyberwar attractiveness
- Hacktivism
  - What is Hacktivism?
  - Ethics and culture of Hacktivists
  - Hacktivist Groups
    - Anonymous
    - WikiLeaks

Cyberwarfare and Hacktivism - References

- Speech by State Department legal adviser Harold Koh at a U.S. Cyber Command interagency legal conference in Fort Meade, Maryland (Sep 2011)
  - "[C]yberactivities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force," he said, and "if the physical consequences of a cyberattack work the kind of physical damage that dropping a bomb or firing a missile would, that cyberattack should equally be considered a use of force." A U.S. response to cyberactivities would not have to take place in cyberspace as long as the response "meets the requirements of necessity and proportionality," he said.
- Libicki, M.C., 2009. *Cyberdeterrence and cyberwar*. Rand Corporation.
  - Appendix A - What Constitutes an Act of War in Cyberspace?
- Stefan Wray, Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics, 1998
- Steve Levy, Hackers: Heroes of the Computer Revolution, 1984
- C. Fuchs, The Anonymous Movement in the Context of Liberalism and Socialism, 2013
- W. H. Wong, P. A. Brown, "E-Bandits in Global Activism: WikiLeaks, Anonymous, and the Politics of No One", 2013