CYBER MERCENARIES

When States Exploit the Hacker Community

Cyber Security Researcher

Michelle Ribeiro

Trabalhou no UOL e na Microsoft, decidiu se juntar ao lado negro da força e trabalhar com Linux. Formada em Administração e Relações Internacionais, com Mestrado em IR na University of London e especialização no MIT, foi escolhida por Harvard e pela revista 'Foreign Policy' ('Política Externa') como uma dos 20 futuro líderes no campo de segurança cibernética.

Chevening Scholarship

www.chevening.org/brazil

Objectives

1. The risks involved when members of the hacker community act as cyber mercenaries
2. What makes so attracting to States to use cyber mercenaries?
3. How the laws of armed conflict enables this use?
4. Is cyber conflicts a new form of war?

Summary

1. International Security Crash Course
2. The Changing Character of War
3. Laws of Cyber Conflict
4. Case Studies
5. Future Developments

1. INTERNATIONAL SECURITY CRASH COURSE

On War

“Every society has its own characteristic form of war”

(Clausewitz, 1832)

Top Ten Terms

1. Mercenaries
2. Military Forces
3. Anarchy
4. Sovereign State
5. Non-Intervention
6. Intergovernmental Organisations
7. International Law
8. Norms
9. Democratic Peace Theory
10. Raison D'etrê

1. MERCENARIES

Traditionally, mercenaries have been defined as non-nationals hired to take direct part in armed conflicts. The primary motivation is monetary gain rather than loyalty to a Nation-State.

2. MILITARY FORCES

Traditionally, the ultimate symbol of sovereignty is a State's ability to monopolise the means of violence; i.e. to raise, maintain, and use military forces.

3. ANARCHY

The 'ordering principle' of international politics according to realism, and that which defines its structure as lacking any central authority.

4. SOVEREIGN STATES

A State is an entity that is recognised to exist when a government is the supreme political authority of a population residing within a defined territory. The recognition is attributed to other States.

5. NON-INTERVENTION

The principle that external powers should not intervene in the domestic affairs of sovereign States.

6. INTERGOVERNMENTAL ORGANISATIONS

An international organisation in which full legal membership is officially solely open to States and the decision-making authority lies with representatives from governments. Ex: UN, ITU, Mercosul.

7. INTERNATIONAL LAWS

The formal rules of conduct that States acknowledge or contract between themselves.

8. NORMS

Specify general standards of behaviour, and identify the rights and obligations of States.

9. DEMOCRATIC PEACE THEORY

A theory which posits that democracies are hesitant to engage in armed conflict as democratic leaders are forced to accept culpability for war losses to a voting public. Democracies usually have internal institutions that makes the use of force the last resource.

10. RAISON D'ETRÊ

According to the Realist school of thought, the predominant reason of the State is to SURVIVE.

International Security Timeline

962-1648

Age of Empires

The local lord, the Holy Roman Emperor, the Pope were the first ‘sovereigns’, followed by the rise of royal power, in Europe.

1648-1871

Treaty of Westphalia

Recognition of the principle of State sovereignty. Birth of the modern State system. American and French Revolution. Rise of the United States and Germany

1914-1945

First & Second World War

The fall of the last empires. 30 years of world instability and rivalry. International Organisations (League of Nations and United Nations)

1947-2012

The Age of New Wars

Cold War, Liberation Wars in Africa, Fall of the Soviet Union, ongoing War on Terror (Iraq & Afghanistan)

2012-Today

Cyber War?

2007: Cyber attacks against Tallinn. 2012: Stuxnet. Cyber Pearl Harbor?

The Age of Empires

International Security Timeline

962-1648

Age of Empires

The local lord, the Holy Roman Emperor, the Pope were the first ‘sovereigns’, followed by the rise of royal power, in Europe.

1648-1871

Treaty of Westphalia

Recognition of the principle of State sovereignty. Birth of the modern State system. American and French Revolution. Rise of the United States and Germany

1914-1945

First & Second World War

The fall of the last empires. 30 years of world instability and rivalry. International Organisations (League of Nations and United Nations)

1947-2012

The Age of New Wars

Cold War, Liberation Wars in Africa, Fall of the Soviet Union, ongoing War on Terror (Iraq & Afghanistan)

2012-Today

Cyber War?

2007: Cyber attacks against Tallinn. 2012: Stuxnet. Cyber Pearl Harbor?

The Treaty of Westphalia

International Security Timeline

962-1648

Age of Empires

The local lord, the Holy Roman Emperor, the Pope were the first ‘sovereigns’, followed by the rise of royal power, in Europe.

1648-1871

Treaty of Westphalia

Recognition of the principle of State sovereignty. Birth of the modern State system. American and French Revolution. Rise of the United States and Germany

1914-1945

First & Second World War

The fall of the last empires. 30 years of world instability and rivalry. International Organisations (League of Nations and United Nations)

1947-2012

The Age of New Wars

Cold War, Liberation Wars in Africa, Fall of the Soviet Union, ongoing War on Terror (Iraq & Afghanistan)

2012-Today

Cyber War?

2007: Cyber attacks against Tallinn. 2012: Stuxnet. Cyber Pearl Harbor?

First and Second World War

International Security Timeline

962-1648

Age of Empires

The local lord, the Holy Roman Emperor, the Pope were the first ‘sovereigns’, followed by the rise of royal power, in Europe.

1648-1871

Treaty of Westphalia

Recognition of the principle of State sovereignty. Birth of the modern State system. American and French Revolution. Rise of the United States and Germany

1914-1945

First & Second World War

The fall of the last empires. 30 years of world instability and rivalry. International Organisations (League of Nations and United Nations)

1947-2012

The Age of New Wars

Cold War, Liberation Wars in Africa, Fall of the Soviet Union, ongoing War on Terror (Iraq & Afghanistan)

2012-Today

Cyber War?

2007: Cyber attacks against Tallinn. 2012: Stuxnet. Cyber Pearl Harbor?

The Age of New Wars

International Security Timeline

962-1648

Age of Empires

The local lord, the Holy Roman Emperor, the Pope were the first ‘sovereigns’, followed by the rise of royal power, in Europe.

1648-1871

Treaty of Westphalia

Recognition of the principle of State sovereignty. Birth of the modern State system. American and French Revolution. Rise of the United States and Germany

1914-1945

First & Second World War

The fall of the last empires. 30 years of world instability and rivalry. International Organisations (League of Nations and United Nations)

1947-2012

The Age of New Wars

Cold War, Liberation Wars in Africa, Fall of the Soviet Union, ongoing War on Terror (Iraq & Afghanistan)

2012-Today

Cyber War?

2007: Cyber attacks against Tallinn. 2012: Stuxnet. Cyber Pearl Harbor?

Cyber Wars?

2. THE CHANGING CHARACTER OF WAR

New Actors and New Finance

New Actors and New Finance

	Before	Now
Actors	National wars (State vs State)	Nation-States, civil wars and foreign actors
Actors	Military forces	Civilians, criminals, mercenaries and private military companies (PMCs)
Finance	National treasure or taxes	Black market of resources, expat community, great powers (US, Russia, Saudi Arabia)

New Goals and New Targets

New Goals and New Targets

	Before	Now
Goals	Territory	Resources (Oil, diamonds, etc)
Targets	Military forces (Away from the population. WWII starts to change this pattern. Aerial bombing	Population control using terror (Child soldiers, sexual violence, random killings, etc)


NETFLIX
BEASTS OF NO NATION

Cyber Wars

Estonia (2007)

Cyber attacks against Estonia (2007)

When Tallinn's government decide to take back the decision to remove the Red Army Soldier Statue, pressioned by Moscow, riots took the streets. Estonia then suffered a month of cyber attacks against its infrastructure.

The Russian authorities denied their involvement and in the face of forensic evidence that suggested that Moscow was indeed behind the attacks against Estonia, Kremlin officials attributed the actions to a nationalist youth organisation called Nashi and pronounced the crime solved.

Cyber Wars

	New Wars	Cyber Wars
Actors	Nation-States, civil wars and foreign actors	Conflicts within Estonia with Russia engagement
Actors	Civilians, criminals, mercenaries and private military companies (PMCs)	Estonian military force, NATO, ethnic Russians (Nashi), cyber criminals, hackers
Finance	Black market of resources, expat community, great powers (US, Russia, Saudi Arabia)	Cyber crime against banks and other institutions
Goals	Resources (Oil, diamonds, etc)	Initially, identity but also political and economic
Targets	Population control using terror (Child soldiers, sexual violence, random killings, etc)	Coercion: Digital infrastructure impairment for a month

Cyber Mercenaries allows Plausible Deniability

Plausible Deniability

The ability of people (typically senior officials in a formal or informal chain of command) to deny knowledge of or responsibility for any damnable actions committed by others in an organizational hierarchy because of a lack of evidence that can confirm their participation, even if they were personally involved in or at least willfully ignorant of the actions.

(Wikipedia)

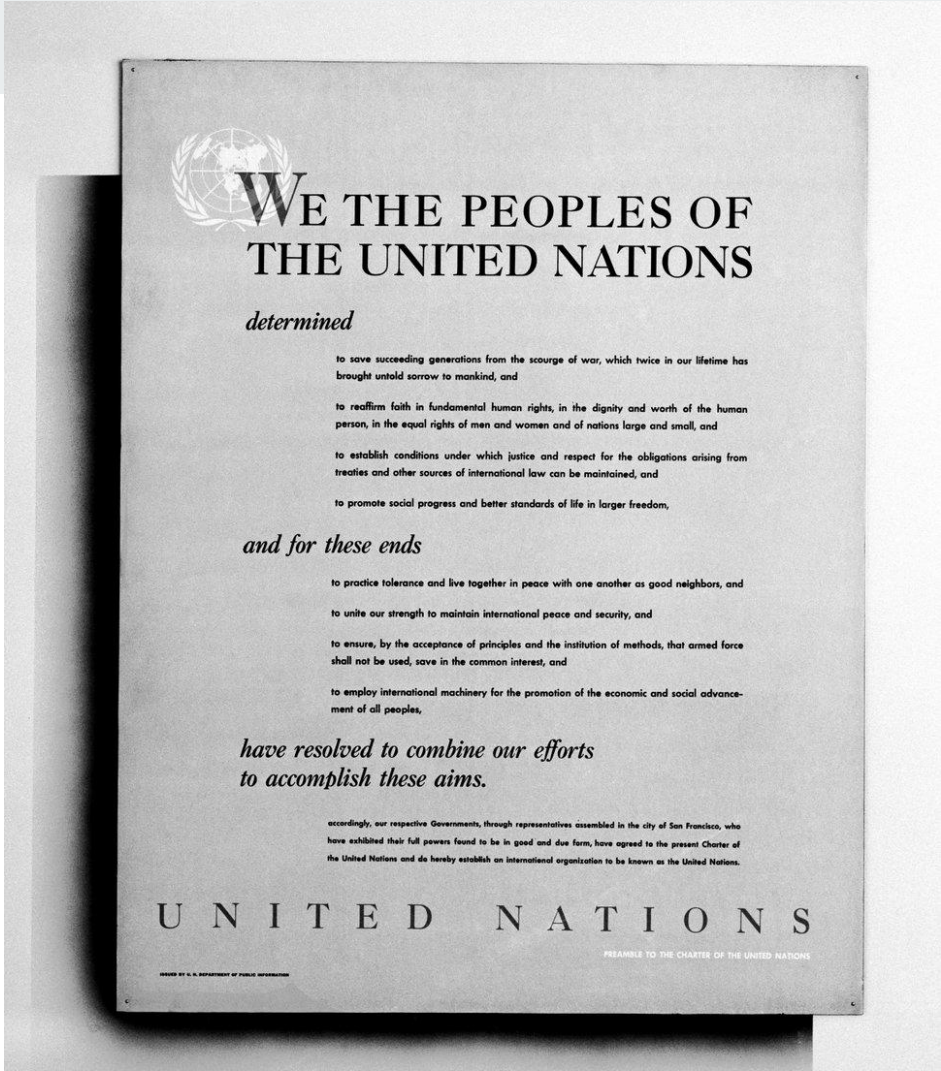
The Attribution Question

Attribution must consider not only technical (factual) but also legal and political concepts.

3. LAWS OF CYBER CONFLICT

1945 UN Charter

As a response to the World War I and World War II



1945 UN Charter

Article 2 (1): The fundamental role of “sovereign equality”.

Article 2 (4): The importance of refraining from “the threat or use or force” against the **territorial** integrity or **political independence** of any State.

Article 39: The DM procedures for determining “the existence of any threat to the peace, breach of the peace or act of aggression”.

Articles 41 and 42: How to respond to such predicaments with (41) and without (42) armed force

1945 UN Charter - Article 41 and 42

Article 41: The UN Security Council may decide what measures not involving the use of armed force are to be employed - basically sanctions.

Article 42: "*Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.*"

1945 UN Charter - Article 51

Article 51: The UN Security Council acknowledges the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.

1949 Geneva Conventions

1949 Geneva Conventions (Int. Hum. Law)

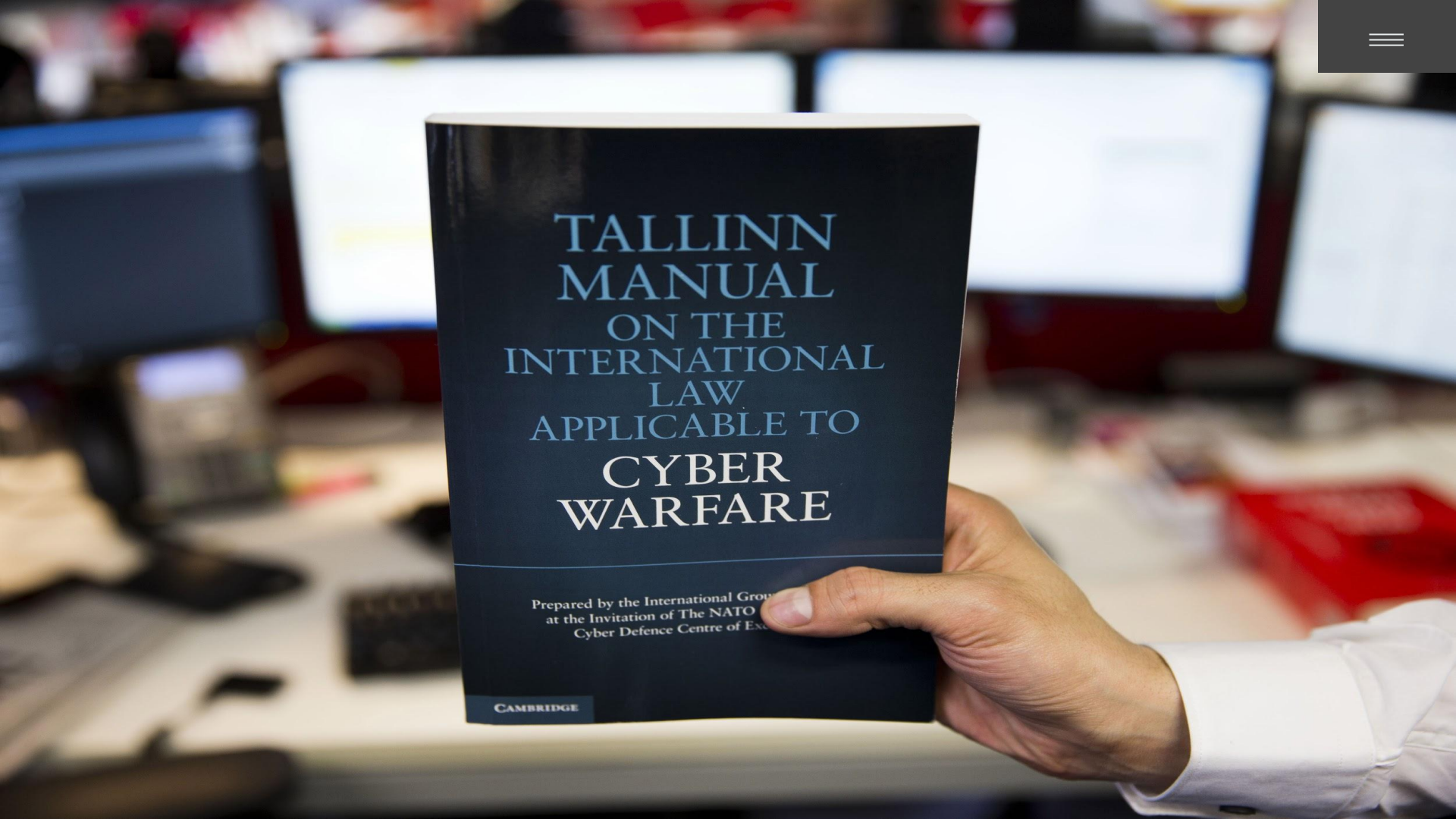
4 basic principles:

1. Distinction;
2. Proportionality;
3. Military Necessity;
4. Unnecessary suffering.

Mercenaries are not recognized as legitimate combatants and do not have to be granted the same legal protections.

Summary

1. The use of force against territorial integrity or political independence is “forbidden”;
2. Force must be used only in cases of threats to international peace and just to restore it;
3. The UN Security Council (US, China, Russia, UK and France + 10) is the decision-maker;
4. Based on unanimity: the veto from one the members prevents decisions;
5. Self-defence is allowed until the UNSC makes a decision;
6. Civilians must be distinct from soldiers. Mercenaries do not have the same rights as soldiers.


TALLINN
MANUAL
ON THE
INTERNATIONAL
LAW
APPLICABLE TO
CYBER
WARFARE
Prepared by the International Grou
at the Invitation of The NATO
Cyber Defence Centre of Ex
CAMBRIDGE

Tallinn Manual 1.0 (2013)

NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), based in Tallinn.

Multiyear project to assess the cyber relevance of the international law governing situations involving the “use of force,” as well as the applicability of international humanitarian law to cyber operations during armed conflicts.

Is Cyber “War” Taking Place, without kinect effect?

Cyber attacks against Estonia (2007)

Tallinn authorities raised the emergency to European Union (EU) officials and requested aid under the Article 5 of the North Atlantic Treaty Organisation (NATO).

NATO technical experts were sent to Tallinn to assist the Estonian government but no military action was taken.

Countermeasures were not allowed as the attacks were not ‘ongoing’.

Cyber attacks against Estonia (2007)

Who the attacker really was?

The Russian authorities denied their involvement and in the face of forensic evidence that suggested that Moscow was indeed behind the attacks against Estonia, Kremlin officials attributed the actions to a nationalist youth organisation called Nashi and pronounced the crime solved.

The right of self-defense would apply only if the perpetrator was a State.

Cyber attacks against Estonia (2007)

Was this cyber offensive an act of war? Could Estonia respond with military force?

The cyber attacks were not 'armed' in a classical manner, considering that physical force and thus destruction and death were not involved

However, they were clearly planned to exploit vulnerabilities and achieve a defined political goal, particularly as they took place in concert with diplomatic pressure from the Kremlin. Political independence?


2016
American Elections

The nature of cyber attacks creates a grey area that makes distinctions difficult.

4. CASE STUDIES

Cyber Mercenaries

The Scapegoat

Study Cases


Canada
Karim Baratov


Syria
Ahmed Umar Agha


Ukraine
Dmitri Golubov

Canada

Karim Baratov

Cyber mercenary for the Russian Federal Security Service (FSB).

The officer who handled him commission hacks on 80 targets in all, including people in other Russian agencies, and government officials in neighboring Eastern European nations.

Cracked more than 11,000 accounts in Russia and the US.

5 years in prison and $250,000 fine for Yahoo breaches.

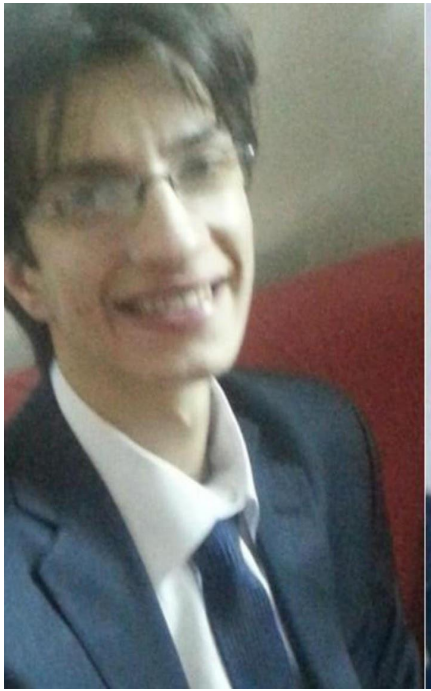
Syria

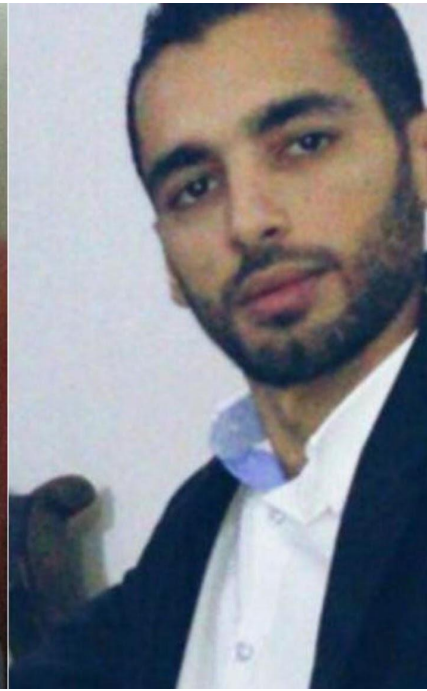
Ahmed Umar Agha

Current or former members of the Syrian Electronic Army;

US authorities have charged Ahmad Umar Agha, 22, Firas Dardar, 27 and Peter Romar, 36 (Germany), with multiple criminal conspiracy;

FBI offers a reward of US$100,000 for information. Romar was arrested in 2016 and extradited to the US.





Ukraine

Dmitri Golubov

Wanted by U.S. law enforcement as a top cyber criminal accused of credit-card fraud;

Briefly imprisoned in 2005 “until two influential Ukrainian politicians convinced a judge to toss out the case;

After founding the Internet Party of Ukraine in 2007, Golubov has been a member of the Ukrainian Parliament since 2014;

As a politician, he has automatic immunity from prosecution for criminal activities under Ukrainian law. Holds more than 4,000 Bitcoins

FBI Cyber's Most Wanted

https://www.fbi.gov/wanted/cyber

How to protect yourself?

Contract with a trusted organisation

5. FUTURE DEVELOPMENTS

The Search for Common Ground

United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications (2004 - 2017)

The fundamental divide between Western States versus Russia, China and others about what constitutes a cyber attack:

CIA triad vs Sovereignty

Cyber Norms are “Processes” instead of “Products”

Back to square zero: involvement of different actors (civil society, academia, think tanks, etc) to construct the social reality around cyber thinking.

Problems to solve

1. Are cyber attacks an act of war?

   What defines cyber conflicts (non-authorised access vs foreign influence)?

2. How to dissuade States from using cyber mercenaries?

3. How to distinguish a cyber mercenary from an intelligence officer from a hacker?

4. Is it perfect attribution possible or should we be happy with evidences?

The Global Commission on the Stability of Cyberspace

Wuzhen World Internet Conference

Digital Geneva Convention

Summary

1. International Security Crash Course
2. The Changing Character of War
3. Laws of Cyber Conflict
4. Case Studies
5. Future Developments

Recommended Books

The following books comprises the cyber security canon, from a political point of view:

01 | Betz, D and Tim Stevens - Cyberspace and the State

02 | Rid, T - The Cyber War will not Take Place

03 | Kello, K - The Virtual Weapon and the International Order

04 | Segal, A - The Hacked World Order

05 | Maurer, T - Cyber Mercenaries

Thank you!

www.mribeiro.uk
twitter.com/michelleribeiro