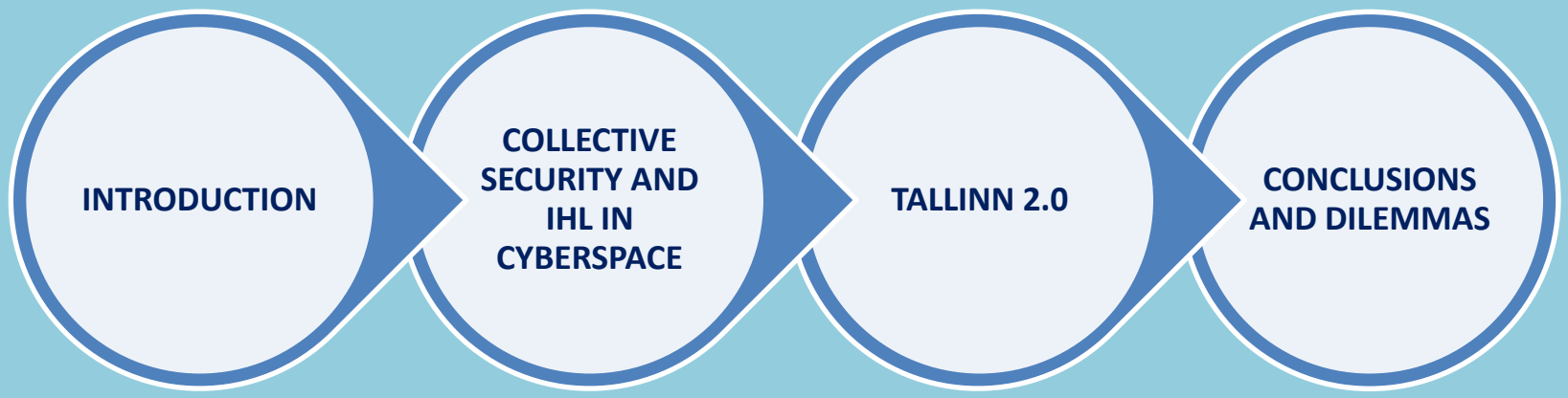
CYBER LAW AND IHL: HIGHLIGHTS AND DILEMMAS

Deborah Housen-Couriel, Adv.

6 September 2017


INTRODUCTION
COLLECTIVE SECURITY AND IHL IN CYBERSPACE
TALLINN 2.0
CONCLUSIONS AND DILEMMAS

(1) INTRODUCTION

TOPICS IN CYBER LAW: A DEVELOPING ARENA OF INTERNATIONAL LAW AND REGULATION

(1) COLLECTIVE SECURITY REGIME AND IHL IN CYBERSPACE

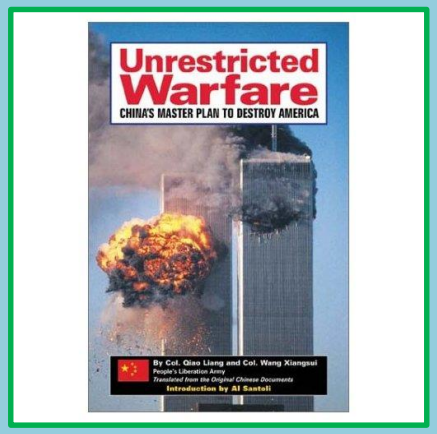
(2) INTERNATIONAL TREATIES

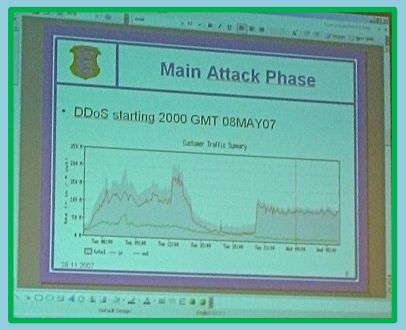
(3) REGIONAL ARRANGE-MENTS

(4) INTERNET GOVERNANCE

(5) CYBER-ENABLED TERRORISM

CYBER ATTACKS ARE GAME CHANGERS FOR IHL

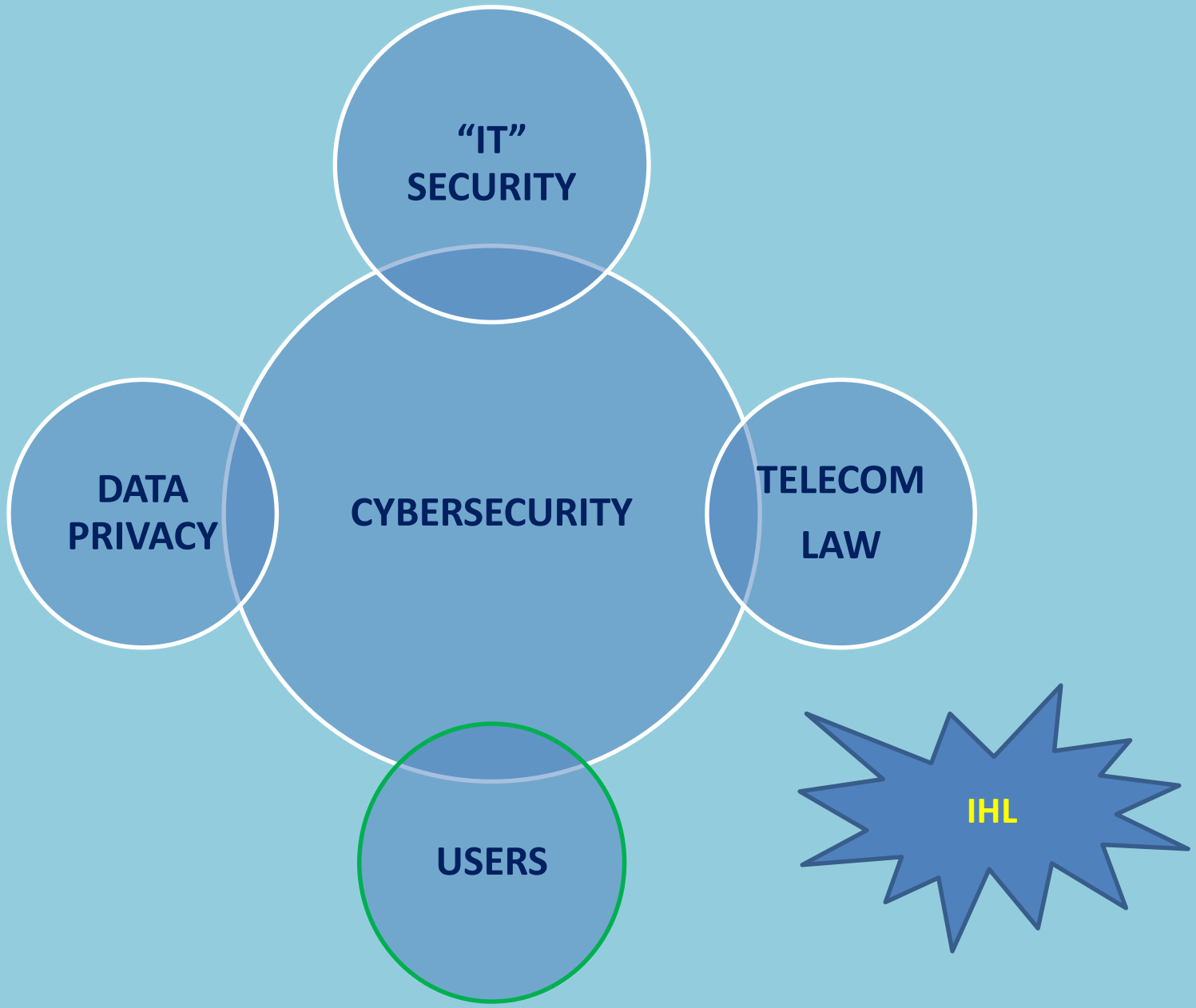




LEGAL CHALLENGES

1. • WHO'S RESPONSIBLE FOR DETERMINING LEGAL NORMS ON THE INTN'L PLANE?
2. • HOW ARE DEFINITIONS AND NORMS AGREED UPON?
3. • DEALING WITH DIFFICULT ISSUES: ATTRIBUTION, NON-STATE ACTORS, FREEDOM OF EXPRESSION, MULTIPLE ID's
4. • ENFORCEMENT, ENFORCEMENT, ENFORCEMENT

DEFINITIONS



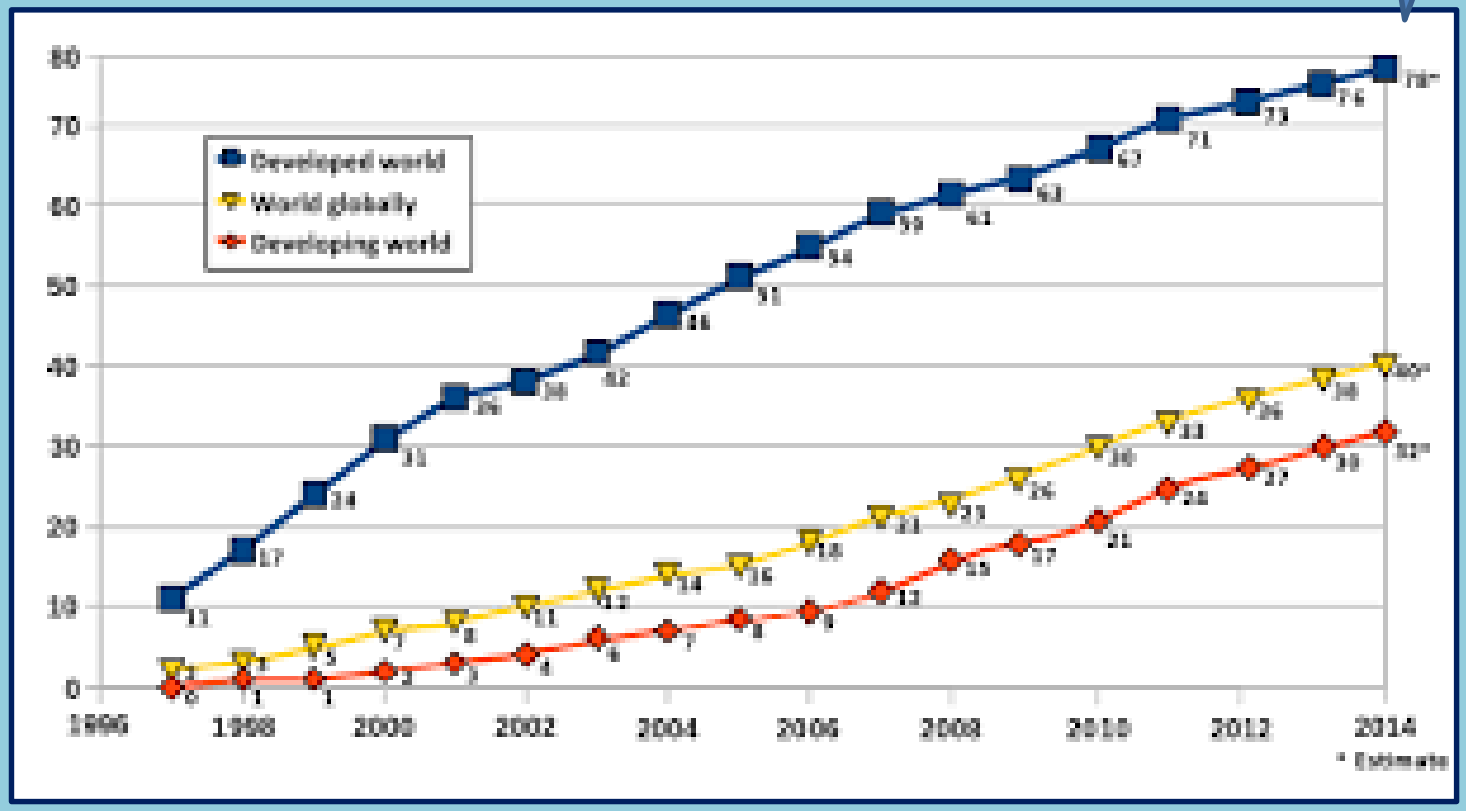
ISRAELI GOV'T RESOLUTION 3611

"Cybersecurity" – policies, security arrangements, actions, guidelines, risk management protocols and technological tools designated to protect cyberspace and allow action to be taken therein.

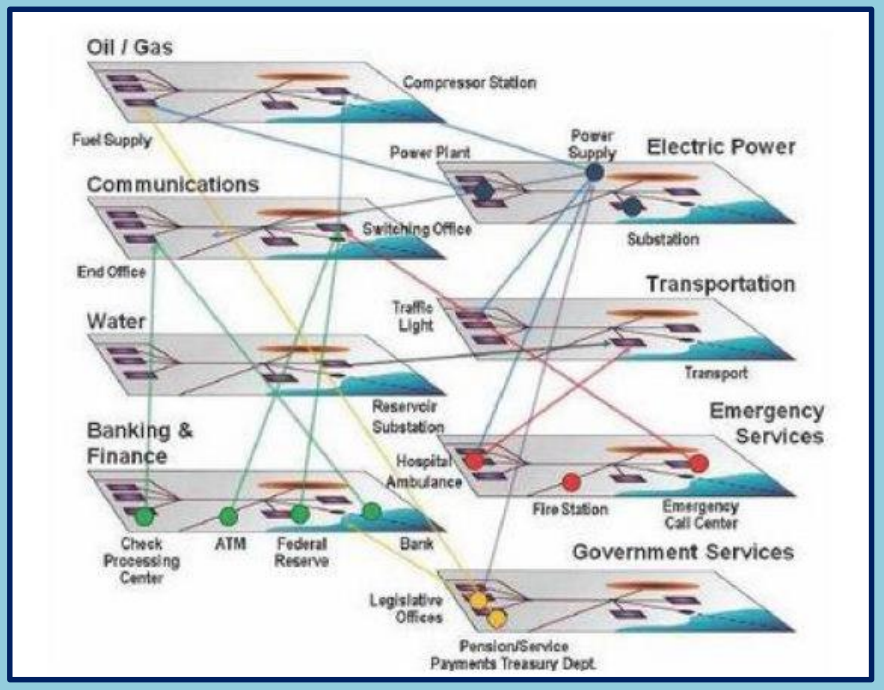
“Cyberspace” – the physical and non-physical domain that is created or composed of part or all of the following components: mechanized and computerized systems, computer and communications networks, programs, computerized information, content conveyed by computer, traffic and supervisory data and those who use such data.

NEW REALITY OF CONNECTEDNESS AND VULNERABILITY

47%
CONNECTED



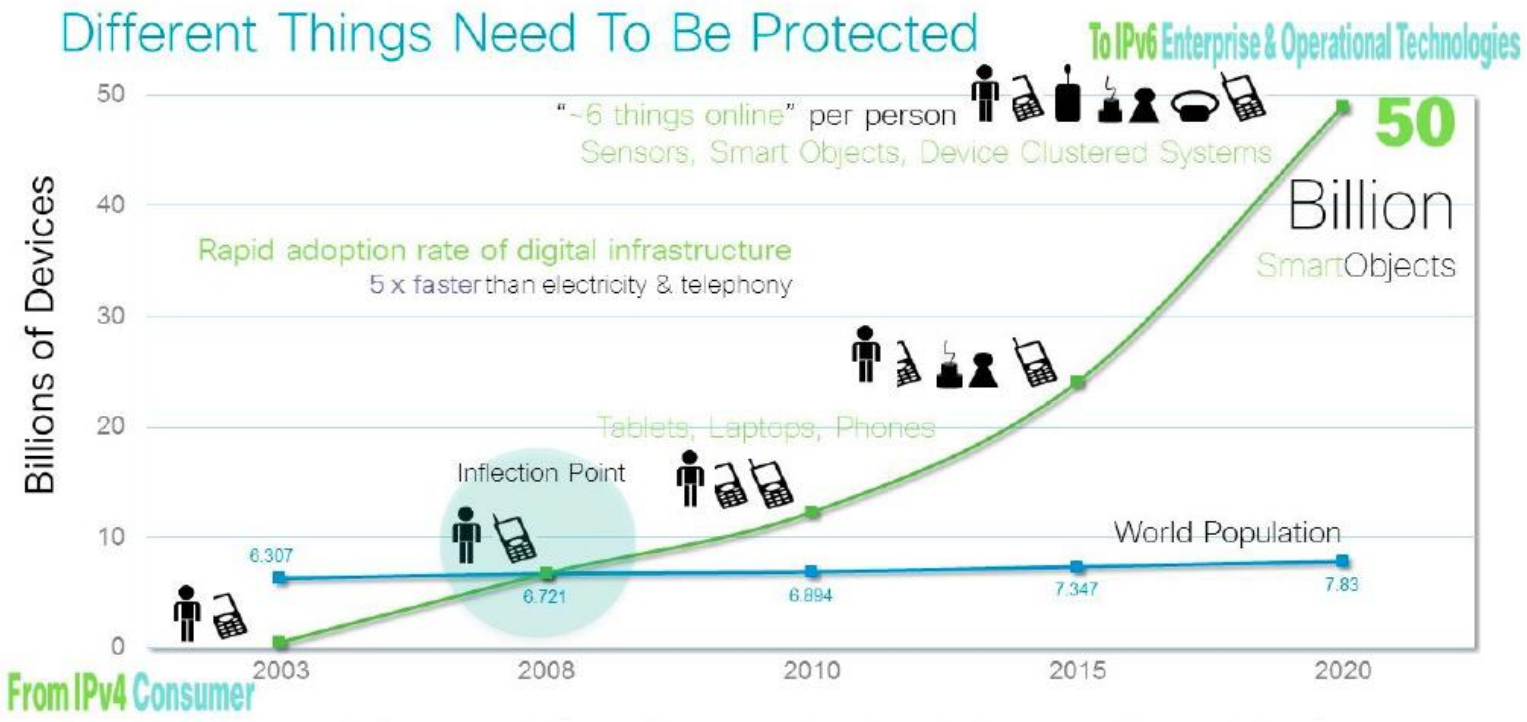
HYPERCONNECTIVITY > HYPER-VULNERABILITY



DISTINCTION BETWEEN MILITARY AND CIVILIAN?

IHL NORMS APPLICABLE TO MILITARY TARGETING ARE CHALLENGED

Internet of Attacking Things



CASE STUDY: SONY, DECEMBER 2013


00:00
01:31

The New York Times | http://nyti.ms/1z5CZPF

ASIA PACIFIC

U.S. Said to Find North Korea Ordered Cyberattack on Sony

By DAVID E. SANGER and NICOLE PERLROTH DEC. 17, 2014

WASHINGTON — American officials have concluded that North Korea was "centrally involved" in the hacking of Sony Pictures computers, even as the studio canceled the release of a far-fetched comedy about the assassination of the North's leader that is believed to have led to the cyberattack.

Senior administration officials, who would not speak on the record about the intelligence findings, said the White House was debating whether to publicly accuse North Korea of what amounts to a cyberterrorism attack. Sony capitulated after the hackers threatened additional attacks, perhaps on theaters themselves, if the movie, "The Interview," was released.

Officials said it was not clear how the White House would respond. Some within the Obama administration argue that the government of Kim Jong-un must be confronted directly. But that raises questions of what actions the administration could credibly threaten, or how much evidence to make public without revealing details of how it determined North Korea's culpability, including the possible penetration of the North's computer networks.

TECH SONY HACK

White House calls Sony hack a 'serious national security matter'

by TIME @TIME DECEMBER 18, 2014, 2:44 PM EST

Doesn't rule out counterattack

This post is in partnership with Time. The article below was originally published at Time.com.

By Zeke J. Miller, TIME

The White House is treating the massive hack of Sony Pictures Entertainment as a "serious national security matter" and is currently devising a "proportional response" to the cyberattack, Press Secretary Josh Earnest said Thursday.

(2) THE COLLECTIVE SECURITY REGIME AND IHL IN CYBERSPACE

USE OF FORCE >>> IHL

IHL DILEMMAS

DISTINCTION **TARGETING**

NECESSITY

UN 2(4)

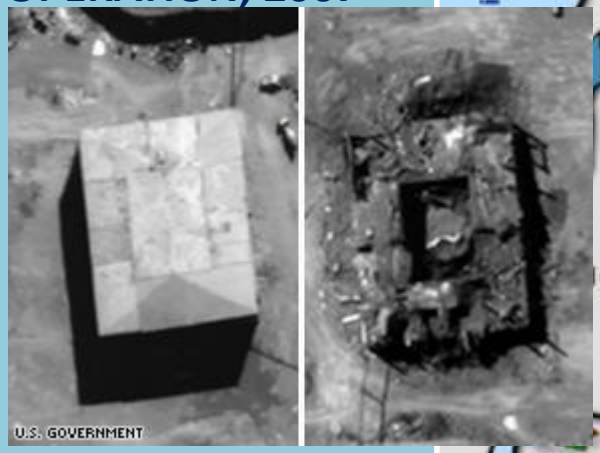
All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

51

- **Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the UN, until the Security Council has taken measures necessary to maintain international peace and security.**

ANTICIPATORY SELF-DEFENSE

BUSTAN OPERATION, 2007



OSIRAK, 1981

Rule 69- Use of Force

A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.

(ICJ Nicaragua 1986)

Rule 71 – Self-Defense

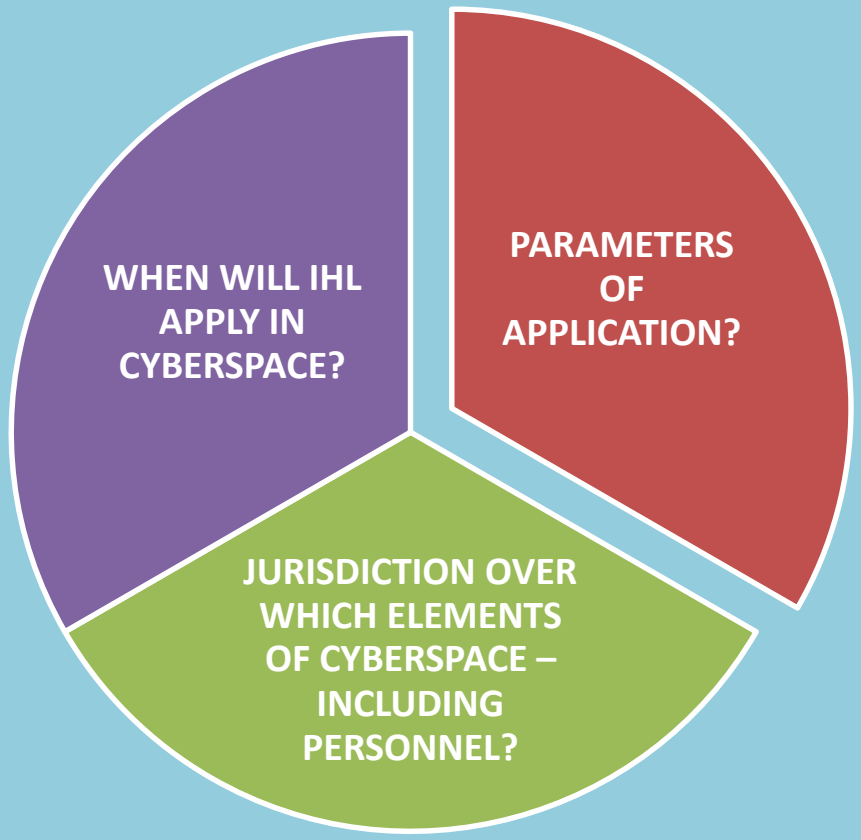
A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense.

(Stuxnet 2010)

CRITERIA FOR “USE OF FORCE”

- severity
- immediacy
- directness
- invasiveness
- measurability of effects
- military character
- state involvement
- presumptive legality

THE KEY QUESTIONS FOR IHL

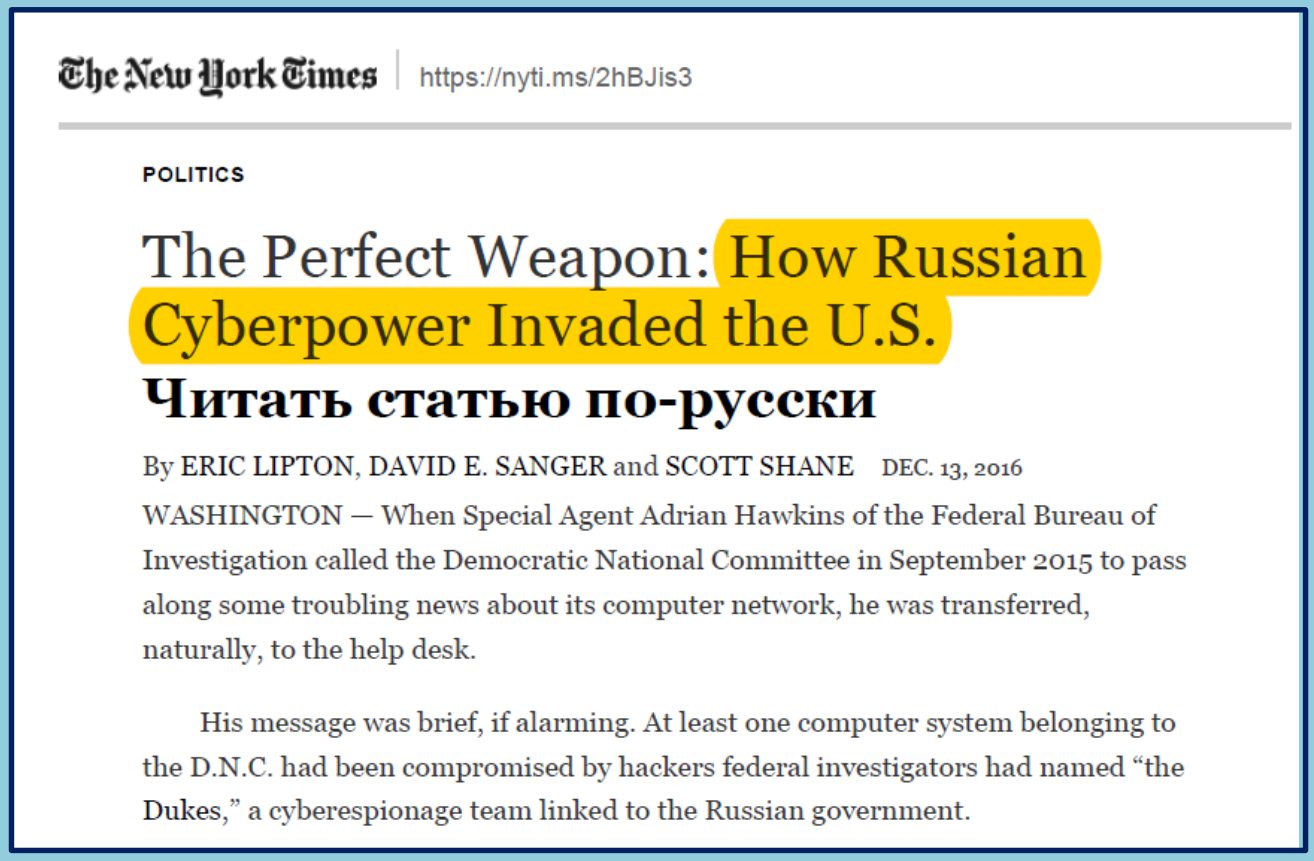


DISTINCTION, TARGETING, NECESSITY

THE PROBLEM OF DISTINCTION

**command chain, uniforms,
weapons carried openly**

THE PROBLEM OF TARGETING



The New York Times | https://nyti.ms/2hBJis3

POLITICS

The Perfect Weapon: How Russian Cyberpower Invaded the U.S.

Читать статью по-русски

By ERIC LIPTON, DAVID E. SANGER and SCOTT SHANE DEC. 13, 2016

WASHINGTON — When Special Agent Adrian Hawkins of the Federal Bureau of Investigation called the Democratic National Committee in September 2015 to pass along some troubling news about its computer network, he was transferred, naturally, to the help desk.

His message was brief, if alarming. At least one computer system belonging to the D.N.C. had been compromised by hackers federal investigators had named "the Dukes," a cyberespionage team linked to the Russian government.

MILITARY NECESSITY - RTS

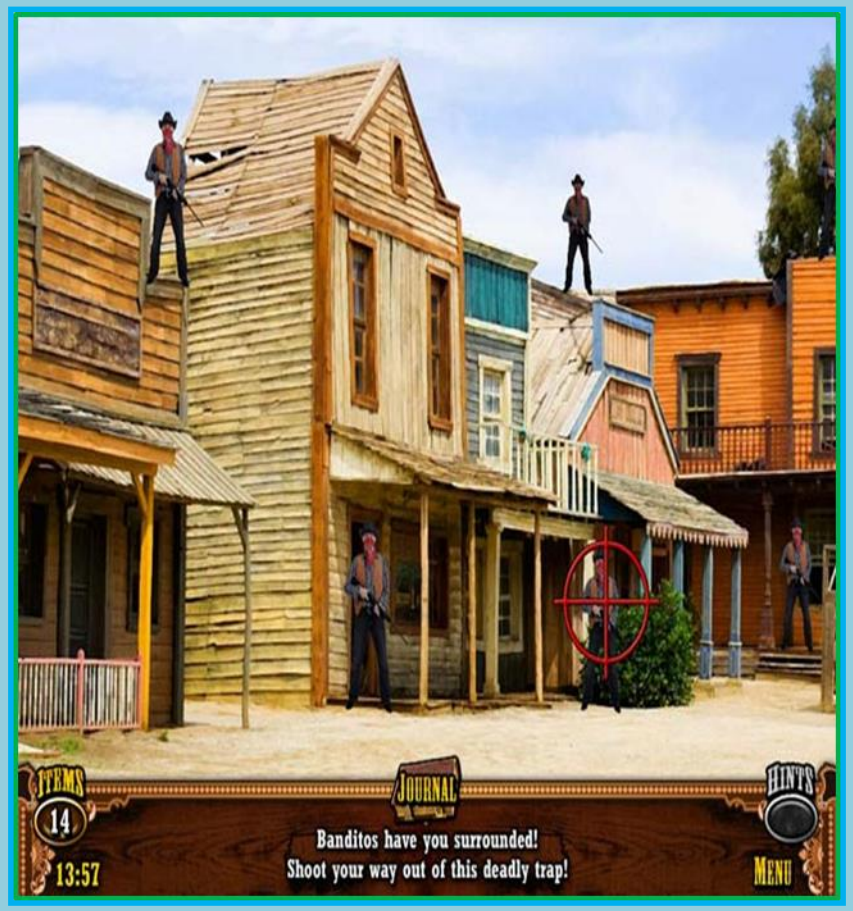
- 23 April 1999 NATO bombed RTS (Radio Television of Serbia) broadcasting station in downtown Belgrade
- Planned attack on a dual-use broadcasting center for military command and control, civilian TV, and satellite broadcasting

- "We need to directly strike at the very central nerve system of Milosovic's regime" – anti-propaganda

- ICTY – no indictments for NATO, yet military necessity questioned

>>> IS CYBER ATTACK PREFERABLE TO KINETIC?

NEW TOOLS, NEW RULES



United Nations A/70/174

General Assembly

Distr.: General
22 July 2015

Original: English

INTERNATIONAL LAW APPLIES TO CYBERSPACE

Seventieth session
Item 93 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Korea, Russia, Spain, UK, USA

NATO §5

72. Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.


NATO OTAN

NORTH ATLANTIC TREATY ORGANIZATION

Wales Summit Declaration

Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales

Press Release (2014) 120 Issued on 05 Sep. 2014 | Last updated: 29 Sep. 2014 09:56

NATO Weighs Making Cyber Wartime Domain

Aaron Mehta, Defense News *5:27 p.m. EDT June 22, 2016*

(Photo: Peter Macdiarmid, Getty Images)

WARSAW, Poland — July's NATO Warsaw Summit will come with a major focus on cyber-related capabilities, and could conclude with a new definition of cyberspace as a warfighting domain – reinforcing the idea that a cyber-attack on a partner could trigger an Article 5 invocation.

Such an announcement represents the increasing focus of cyber for the alliance at a time when Russia is increasingly focused on asymmetrical warfare to try and weaken the European members, as Western officials have said. That NATO is considering a change in how cyber is handled on a policy level was revealed by a source involved in the planning for next month's summit.

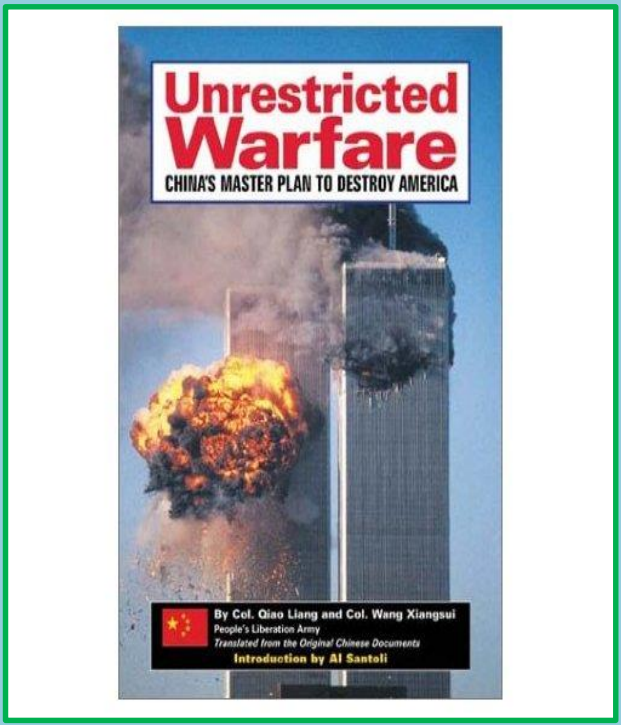
AND YET…

"INFORMATION SECURITY"

- Cyber CODE OF CONDUCT, 2015

-

CHINA: "UNRESTRICTED WARFARE", 1999



"…if the attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis. There is finally the forceful bearing down by the army, and military means are utilized in gradual stages until the enemy is forced to sign a dishonorable peace treaty."

THE GGE THAT WASN'T

Dispute along cold war lines led to collapse of UN cyberwarfare talks

Thirteen years of negotiations came to an abrupt end in June, it has emerged, because of a row over the right to self-defence in the face of attacks

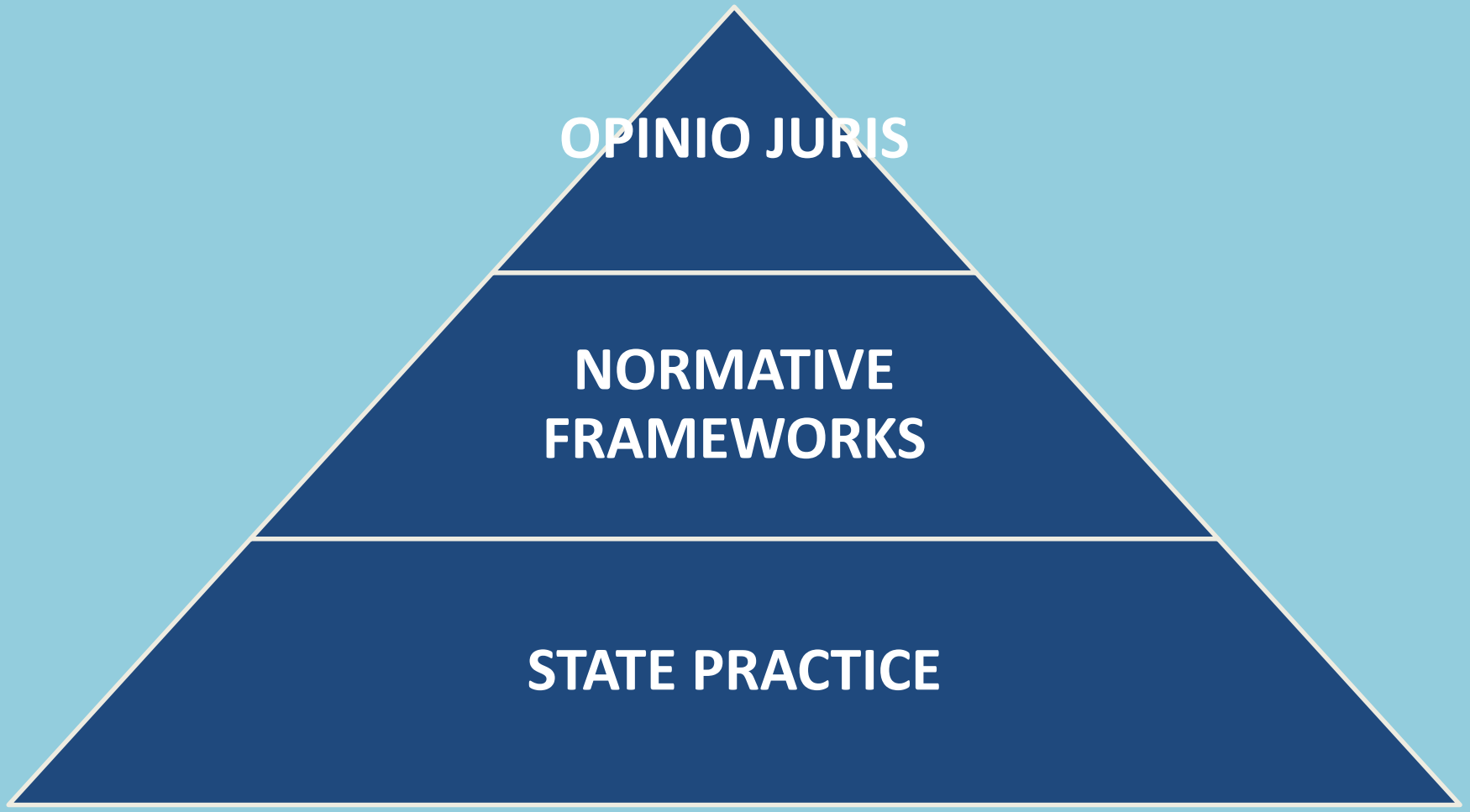
Owen Bowcott Legal affairs correspondent

Wednesday 23 August 2017 01.00 EDT

Thirteen years of negotiations at the United Nations aimed at restricting cyberwarfare collapsed in June, it has emerged, due to an acrimonious dispute that pitted Russia, China and Cuba against western countries.

“Houston, we have a problem.”

WHAT'S ALREADY IN PLACE?



2009-2015

► UN GGE

2013

► OSCE CBMs

► EUROPOL CYBERCRIME CENTER

► TALLINN 1.0

2014

► AFRICAN UNION TREATY

► NATO SUMMIT

► NET-MUNDIAL

2015

► SCO CODE OF CONDUCT

► UN GGE

► G20 AND NATO COMMUNIQUES

► US-CHINA BILATERAL

► RUSSIA-CHINA BILATERAL

2017

► POLICY STATEMENTS BY US DoD, UK, Netherlands, Israel

► G7

► NATO

► TALLINN 2

CONVENTION ON CYBERCRIME, 2001

THE DEPARTMENT OF DEFENSE CYBER STRATEGY

April 2015

Response: The United States has been clear that it will respond to a cyberattack on U.S. interests through its defense capabilities. The United States has articulated this declaratory policy in the 2011 United States *International Strategy for Cyberspace*, in the Department of Defense Cyberspace Policy Report to Congress of 2011, and through public statements by the President and the Secretary of Defense. The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law.

“A SERIOUS, ORGANISED CYBER ATTACK ON ESSENTIAL FUNCTIONS OF THE STATE COULD CONCEIVABLY BE QUALIFIED AS AN ‘ARMED ATTACK’ WITHIN THE MEANING OF ARTICLE 51 …IF IT COULD OR DID LEAD TO SERIOUS DISRUPTION OF THE FUNCTIONING OF THE STATE OR SERIOUS AND LONG-LASTING CONSEQUENCES FOR THE STABILITY OF THE STATE.”

PARLIAMENT, 2011

בלמ"ס

לשכת הרמטכ"ל

אסטרטגיית צה"ל

אב התשע"ה

אוגוסט 2015

בניית יכולת במרחב הסייבר

25. המרחב הקיברנטי הוא מרחב לחימה נוסף. במרחב זה יבוצעו פעולות הגנה, איסוף והתקפה. בניין הכוח של צה"ל במרחב זה יתבסס על פעולות אלה:

א. הקמת זרוע הסייבר שתהווה מפקדה ראשית הכפופה לרמטכ"ל להפעלה ובניין הכוח של יכולות הסייבר בצה"ל ותהיה אחראית לתכנון ולמימוש המערכה במרחב הסייבר.

ב. פיתוח יכולות טכנולוגיות להגנה בסייבר על כל המערכות המבצעיות ויכולות הגנה על מערכות מסייעות (מע' כ"א, לוגיסטיקה).

מאמץ בסייבר במסגרת מצב מלחמה או חירום יתמוך במאמצי ההגנה וההתקפה בכל רמות הלחימה – אסטרטגי, אופרטיבי וטקטי.

ההגנה בסייבר במלחמה ובחירום חיונית כדי לאפשר הן את הפעלת מוסדות המדינה בעימות והן כדי לאפשר פעולה אפקטיבית של צה"ל, המבוססת על רשתיות.

A Digital Geneva Convention

1. **No targeting of tech companies, private sector, or critical infrastructure**

2. **Assist private sector efforts** to detect, contain, respond to, and recover from events

3. **Report vulnerabilities to vendors** rather than to stockpile, sell or exploit them

4. **Exercise restraint in developing cyber weapons** and ensure that any developed are limited, precise, and not reusable

5. **Commit to nonproliferation** activities to cyberweapons

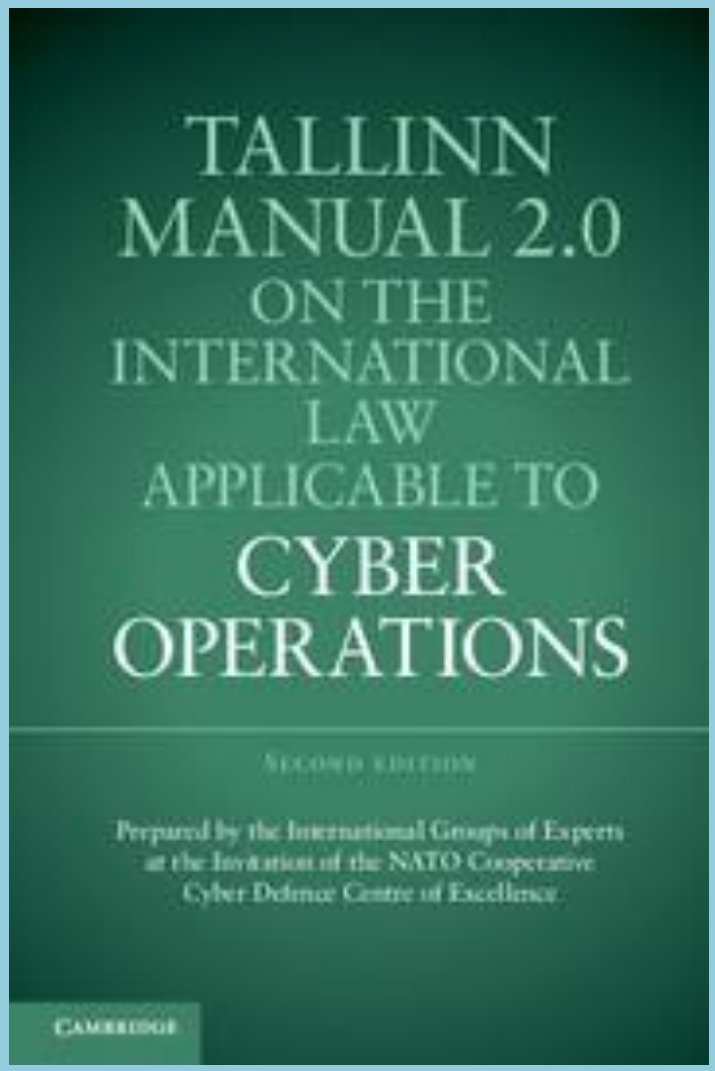
6. **Limit offensive operation** to avoid a mass event

- Microsoft President Brad Smith, February 2017

(3) TALLINN 2.0

2017

- **INTERNATIONAL LAW AND COLLECTIVE SECURITY APPLY**
- **STATE RESPONSIBILITY OVER INFRASTRUCTURE**
- **PROCESS: NOT STATES (FOR GOOD REASON)**
- **LEADING EXPERT AUTHORITIES**
- **STATES' DE FACTO ACKNOWLEDGEMENT**



Tallinn 2.0 Topics

- Sovereignty
- Jurisdiction
- Due Diligence
- Prohibition of Intervention
- State Responsibility
- Responsibility of IOs
- Human Rights Law
- Air Law
- Space Law
- Diplomatic Law
- Law Applicable to Peacekeeping Operations
- International Telecommunications Law
- Cyber Operations Not *Per Se* Regulated by International Law
  - Cyber espionage
  - Private sector cyber operations
- Updates to Tallinn 1.0

- THE LEADING NORMATIVE PROCESS
  - "NORMATIVE SENSITIVITIES"
  - INTERNATIONAL LAW APPLIES
    - SCOPE OF T1 AND T2
    - STATES' REACTIONS

RULE 69: “USE OF FORCE”

A CYBER OPERATION CONSTITUTES A USE OF FORCE WHEN ITS SCALE AND EFFECTS ARE COMPARABLE TO NON-CYBER OPERATIONS RISING TO THE LEVEL OF A USE OF FORCE.

(ICJ NICARAGUA 1986)

RULE 92: “CYBER ATTACK”

A CYBER ATTACK IS A CYBER OPERATION, WHETHER OFFENSIVE OR DEFENSIVE, THAT IS REASONABLY EXPECTED TO CAUSE INJURY OR DEATH TO PERSONS OR DAMAGE OR DESTRUCTION TO OBJECTS.

WHAT ABOUT CYBER OPERATIONS AGAINST…

- BANKS AND STOCK EXCHANGES
- GOVERNMENTAL DISASTER WARNING WEBSITES
- SOCIAL SECURITY PAYMENTS
- ELECTORAL SYSTEMS

SETTING A NORMATIVE FRAMEWORK – CONCLUSIONS FROM TALLINN

- INTERNATIONAL LAW OBTAINS IN CYBERSPACE
- STATE AND MILITARY DECLARATIONS
- THE GLOBAL LEGAL CONVERSATION
- IN-DEPTH LEGAL ISSUE ANALYSIS
- SETTING EXPECTATIONS

AND YET…THE GGE THAT WASN'T

Dispute along cold war lines led to collapse of UN cyberwarfare talks

Thirteen years of negotiations came to an abrupt end in June, it has emerged, because of a row over the right to self-defence in the face of attacks

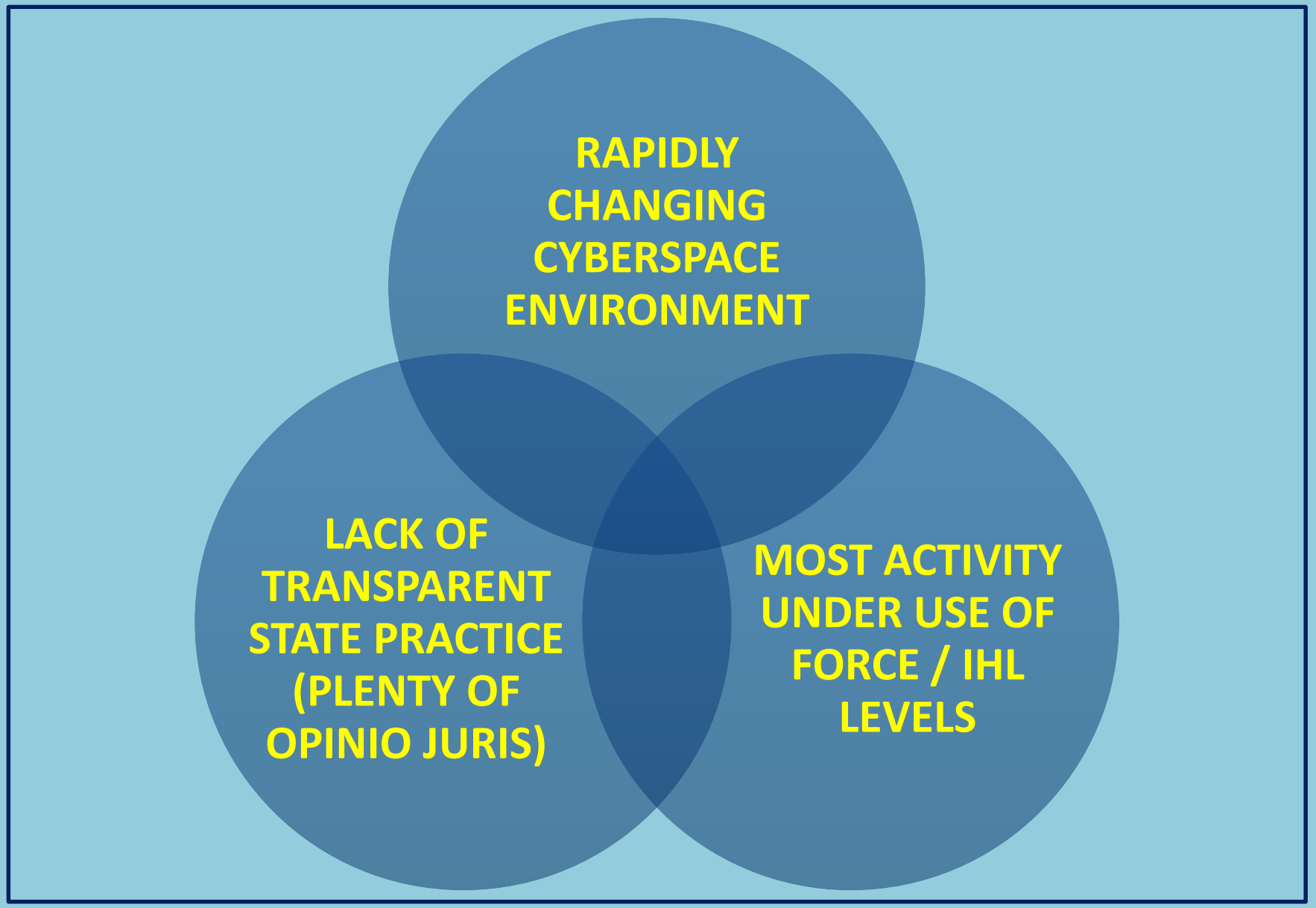
Owen Bowcott Legal affairs correspondent

Wednesday 23 August 2017 01.00 EDT

Thirteen years of negotiations at the United Nations aimed at restricting cyberwarfare collapsed in June, it has emerged, due to an acrimonious dispute that pitted Russia, China and Cuba against western countries.

WHAT ABOUT SONY?

(4) CONCLUSIONS AND DILEMMAS


RAPIDLY CHANGING CYBERSPACE ENVIRONMENT
LACK OF TRANSPARENT STATE PRACTICE (PLENTY OF OPINIO JURIS)
MOST ACTIVITY UNDER USE OF FORCE / IHL LEVELS

“CYBER CANTONIZATION” v. COORDINATED GLOBAL NORMS

THANK YOU.