רגולציה בינלאומית של מרחב הסייבר

אבטחת מידע וסייבר: טכנולוגיה, יזמות עסקית ורגולציה

הפקולטה למשפטים, אוניברסיטת חיפה

סוגיות בדיני סייבר בינלאומיים: מערכת נורמאטיבית מתפתחת והמוסדות שתומכים בהן

(1) מערכת הבטחון הקולקטיבי במרחב הסייבר

(2) אמנות בינלאומיות

(3) הסדרים איזורים

(4) משילות באינטרנט

(5) טרור מקוון

בין הסוגיות המשפטיות המאתגרות

1. • מי אחראי על ההסדרה מבחינת המוסדות הבינלאומיים והמדינתיים – וכיצד להסדיר?
2. • כיצד מפתחים הגדרות יסוד?
3. • התמודדות עם נושאים מהותיים– ייחוס, שחקנים שאינם מדינות, חופש הביטוי
4. • אכיפת נורמות משפטיות במישור הבינלאומי

הגדרות


אבטחת מידע
הגנה על פרטיות מידע
"הגנת סייבר"
דיני תשתיות תקשורת
משתמשים

החלטה 3811

קידום היכולת הלאומית במרחב הקיברנטי

"ביטחון סייבר"-

מדיניות,

מנגנוני אבטחה, פעולות, הנחיות, ניהול סיכונים וכלים טכנולוגיים,

שנועדו להגן על המרחב הקיברנטי ושנועדו לאפשר פעולה בו.

החלטה 3611

"מרחב הסייבר" - המתחם

הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים:

מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן

ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה.

פרשת סוני

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.

האמירה הרגולטורית בתוך ארה"ב

SONY
PICTURES

10202 West Washington Boulevard
Culver City, California 90232-3195

December 8, 2014

Dear SPE Employee:

Sony Pictures Entertainment ("SPE") is writing to provide you with a summary of SPE's prior communications regarding the significant system disruption SPE experienced on Monday, November 24, 2014, as well as to provide you with additional detail.

As you know, SPE has determined that the cause of the disruption was a brazen cyber attack. After identifying the disruption, SPE took prompt action to contain the cyber attack, engaged recognized security consultants and contacted law enforcement.

SPE learned on December 1, 2014, that the security of personally identifiable information that SPE received about you and/or your dependents during the course of your employment may have been compromised as a result of such brazen cyber attack. Although SPE is in the process of investigating the scope of the cyber attack, SPE believes that the following types of personally identifiable information that

(1) מנגנון הבטחון הקולקטיבי במגילת האו"ם

מגילת האו"ם, 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.

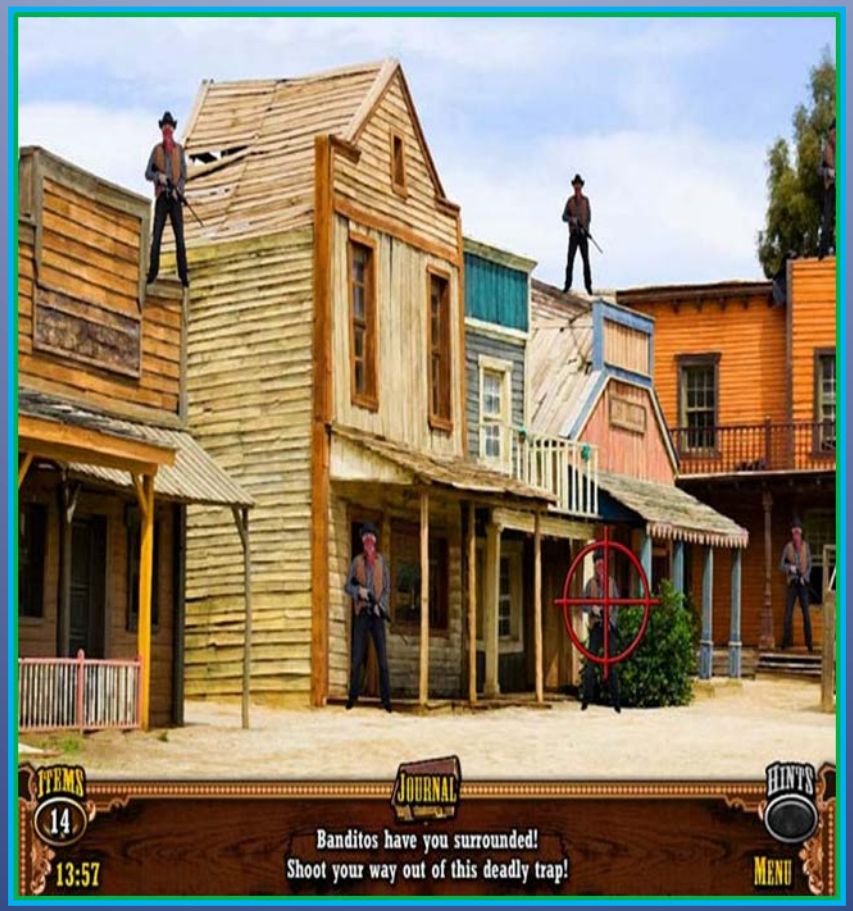
51

- **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.**

מקדימה

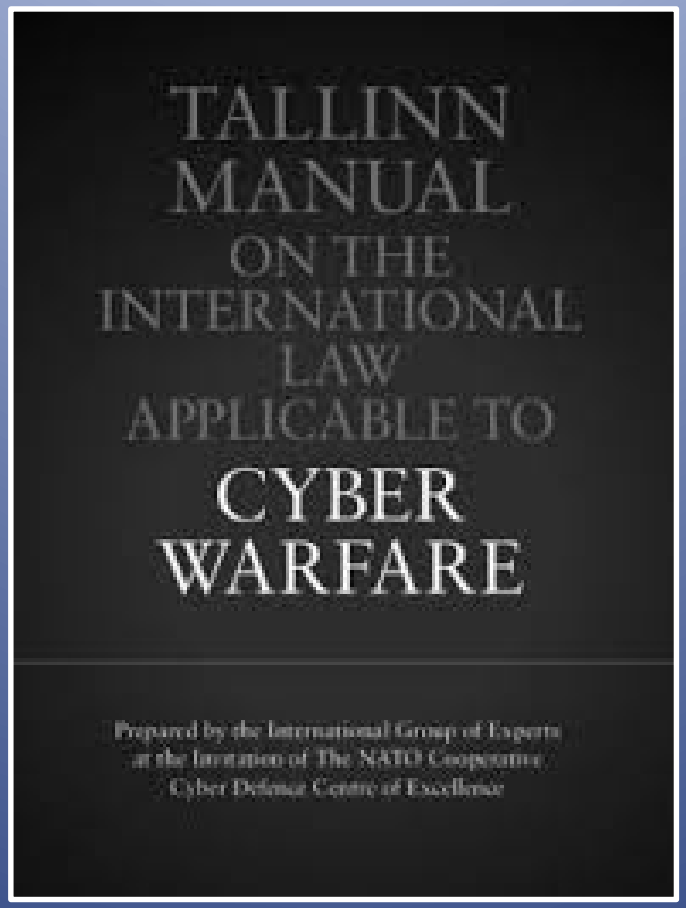

Original Centrifuge Plant
Earth-covered
Underground Bldgs
323,000 sq. feet each
95,000 sq ft Bldg
under construction
Tunnel Entrance
Admin. Bldg.

NEW TOOLS, NEW RULES



“Houston, we have a problem.”

מדריך טאלין, 2013



- התהליך המוביל
במישור הבינלאומי כעת

- בוחן את החלת הדין הבינ"ל במרחב

- היקף
- רגישות לגבולות הדין ("מתקפה" – הסדר הבטחון הקולקטיבי)
- קשב לצרכי מדינות (מנהג)

"מתקפת סייבר"

RULE 30

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.

הגדרת "שימוש בכוח" (כלל 11)

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)

הגנה עצמית (כלל 13)

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)

פרשת סוני?

CIA Eyes Russian Hackers in 'Blackout' Attack

Somebody hacked the Ukrainian power grid just before Christmas—an
U.S. intel analysts are looking toward Moscow for answers.

U.S. intelligence and security agencies are investigating whether Russian government hackers were behind a cyber attack on the Ukrainian power grid last month, multiple sources familiar with the investigation told The Daily Beast.

אין עדיין פרקטיקה – ממשלות ספורות מצהירות מדיניות (הולנד)

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 of the UN Charter 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.

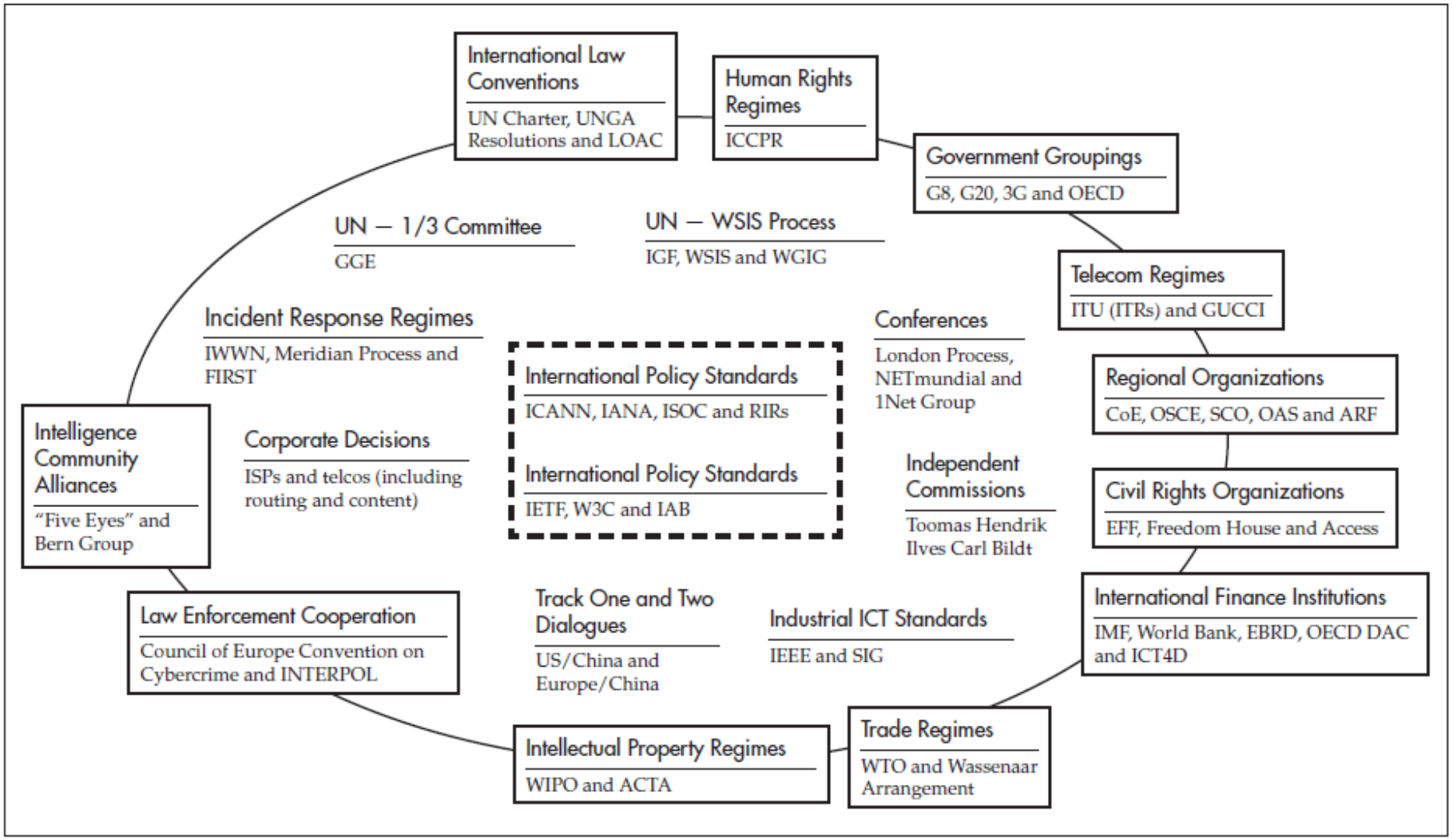
גיבוש המע' הנורמטיבית של בטחון קולקטיבי במרחב -ממצאי התהליך של מדריך טאלין

- המשב"ל ודיני המלחמה אכן חלים במרחב
- הסכמת מדינות וצבאות
- השקת דיון ציבורי בינ"ל שהוא משפטי בעיקר
- ניתוח יסודי של סוגיות וגיבוש הגדרות
- וודאות / ציפיות / קווים אדומים

כיצד פועל המשפט הבינלאומי?

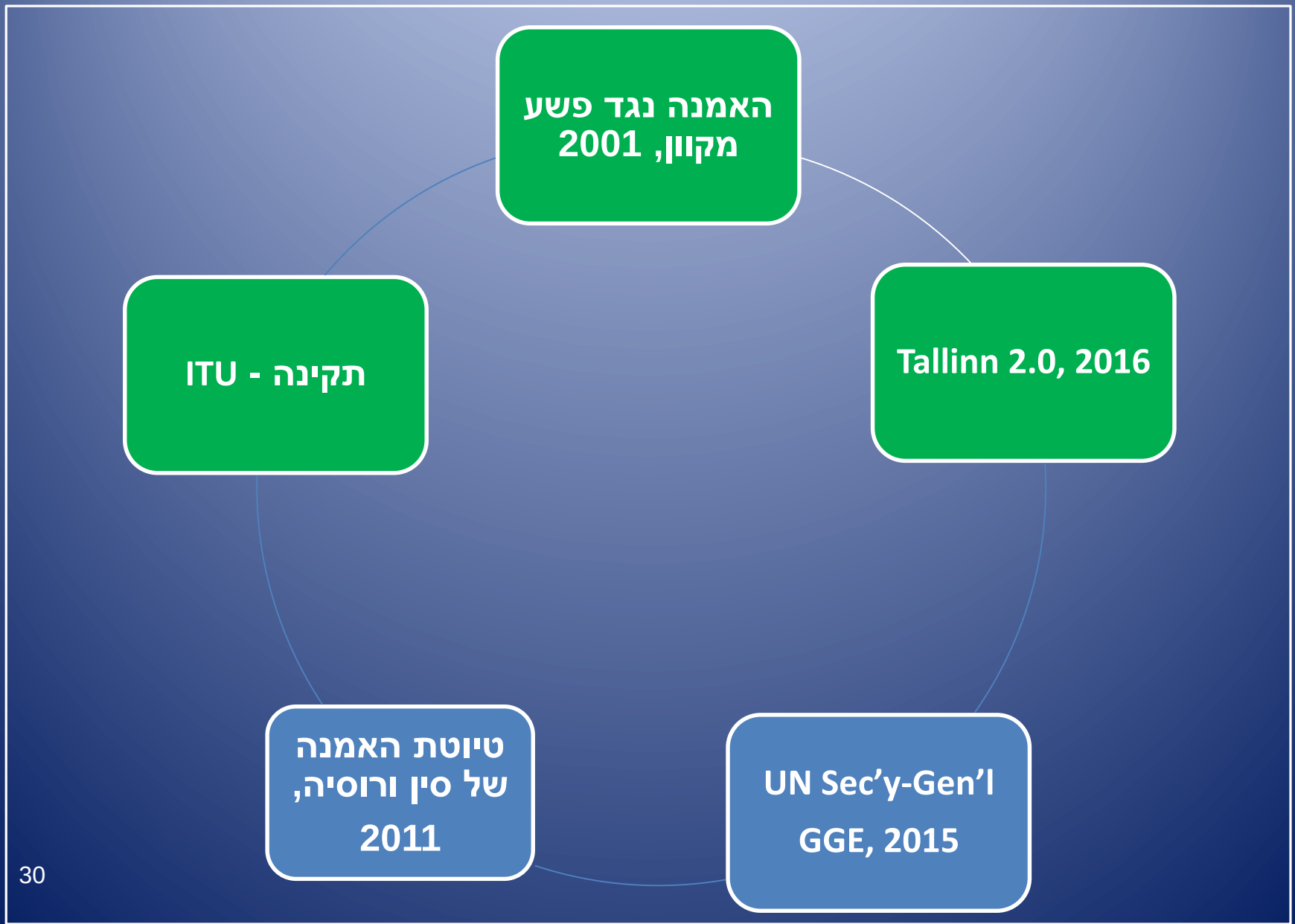
(2) אמנות בינלאומית

Figure 1: The Regime Complex for Managing Global Cyber Activities



Source: Author.

מספר יוזמות רב-צדדיות



אמנת בודפשט, 2001

גישה אסורה למע' מחשב (ס'2)

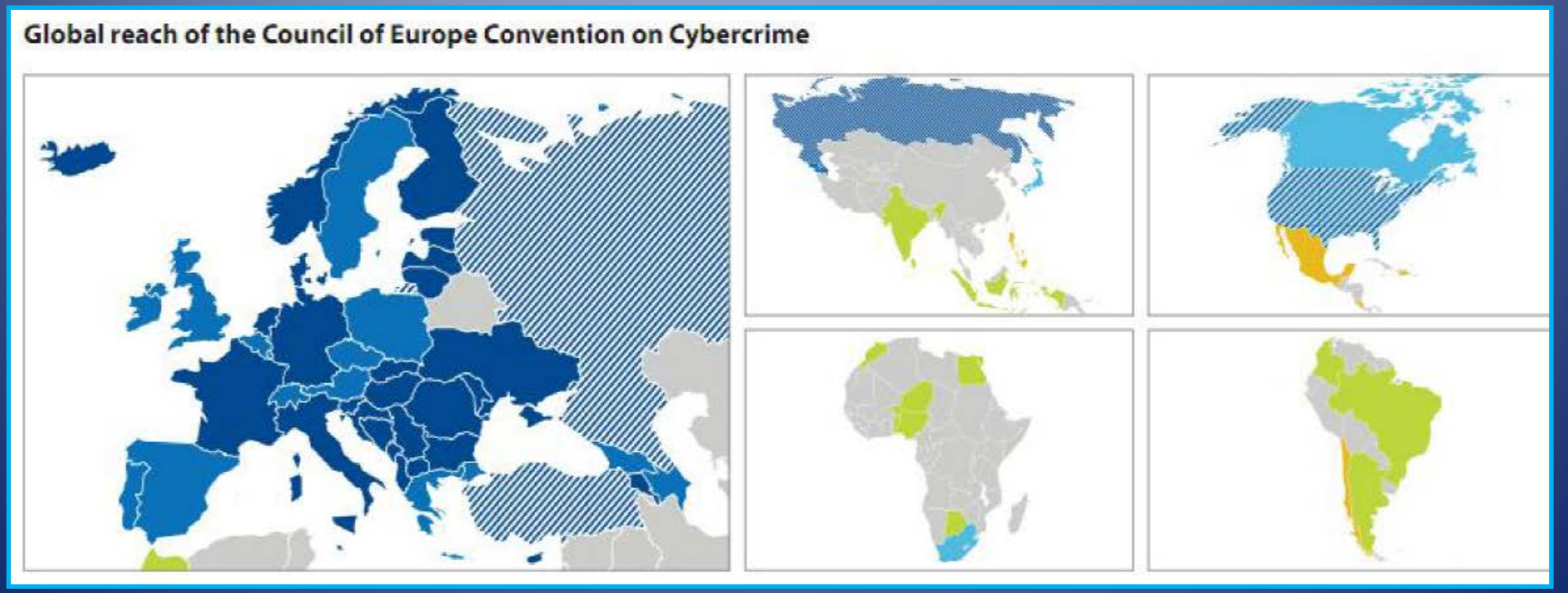
התערבות אסורה בהעברת מידע (ס' 3)

עיוות מידע אסור (ס' 4)

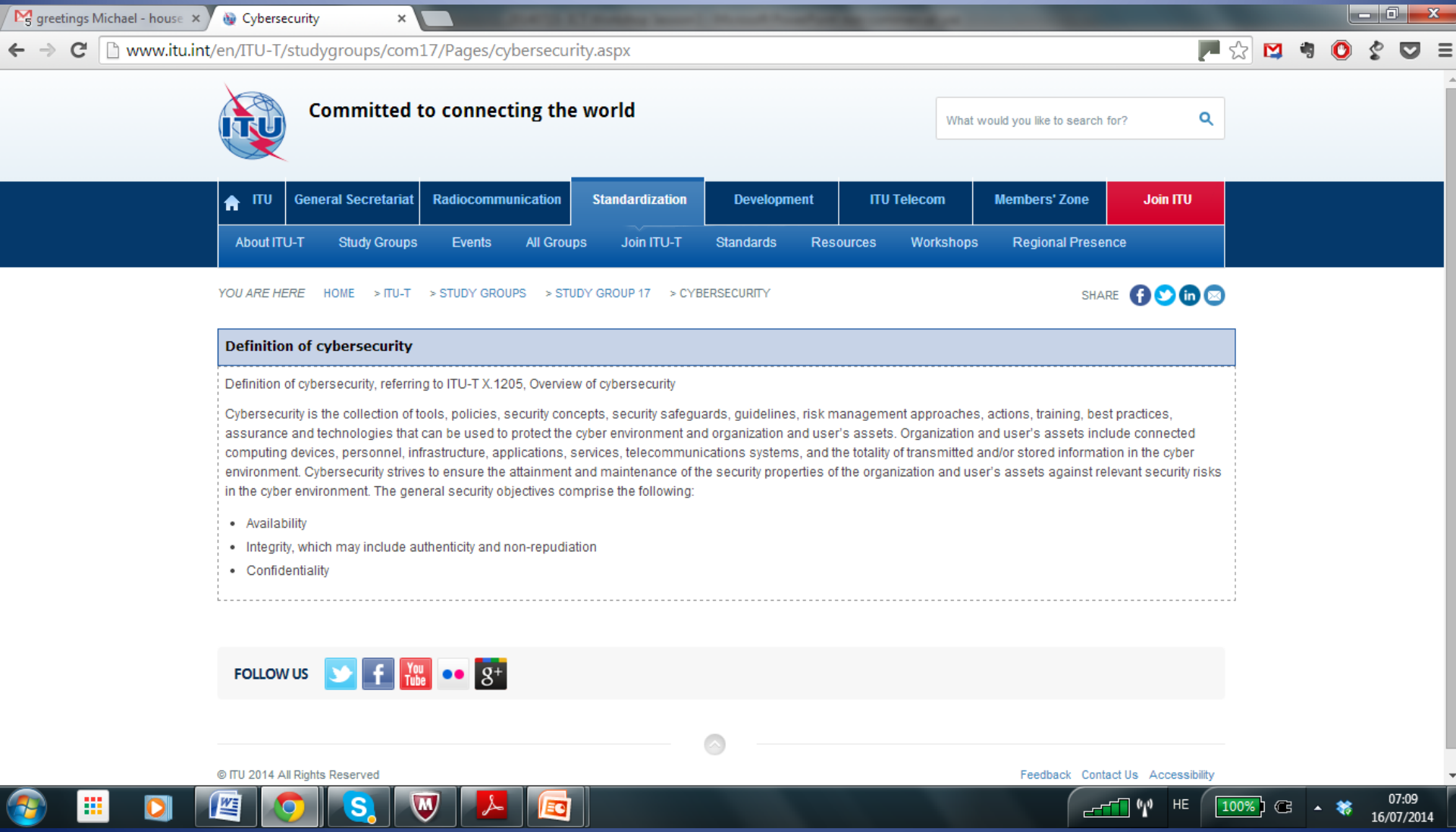
התערבות אסורה במערכות מחשב (ס' 6)

חלק III – תכנים אסורים

רגולציה בהיקף רחב דרך הנורמות באמנת בודפשט



רגולציה דרך תקינה - ITU-T X.1205



Tallinn 2.0 Facts

- **Project hosted by NATO CCD COE 2013-2016**
- **Deepens the analysis of peacetime international law**
  - **Current Rules 1-9**
- **Will result in the second, expanded edition of the Tallinn Manual**

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

(3) הסדרים איזוריים

ס' 5 נאט"ו

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

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE OF THE
EUROPEAN UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 7.2.2013
JOIN(2013) 1 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

Network Directive – "רגולציה אזורית"

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Directive lays down measures to ensure a high common level of network and information security (hereinafter referred to as "NIS") within the Union.

2. To that end, this Directive:

(a) lays down obligations for all Member States concerning the prevention, the handling of and the response to risks and incidents affecting networks and information systems;

(b) creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems;

(c) establishes security requirements for market operators and public administrations.

Privacy Directive -"רגולציה איזורית"

DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 12 July 2002

concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission ([1]),

Having regard to the opinion of the Economic and Social Committee ([2]),

Having consulted the Committee of the Regions,

and privacy for users of publicly available electronic communications services, regardless of the technologies used. That Directive should therefore be repealed and replaced by this Directive.

(5) New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the information society is characterised by the introduction of new electronic

הפסקה!

משילות באינטרנט

INTERNET GOVERNANCE PRINCIPLES

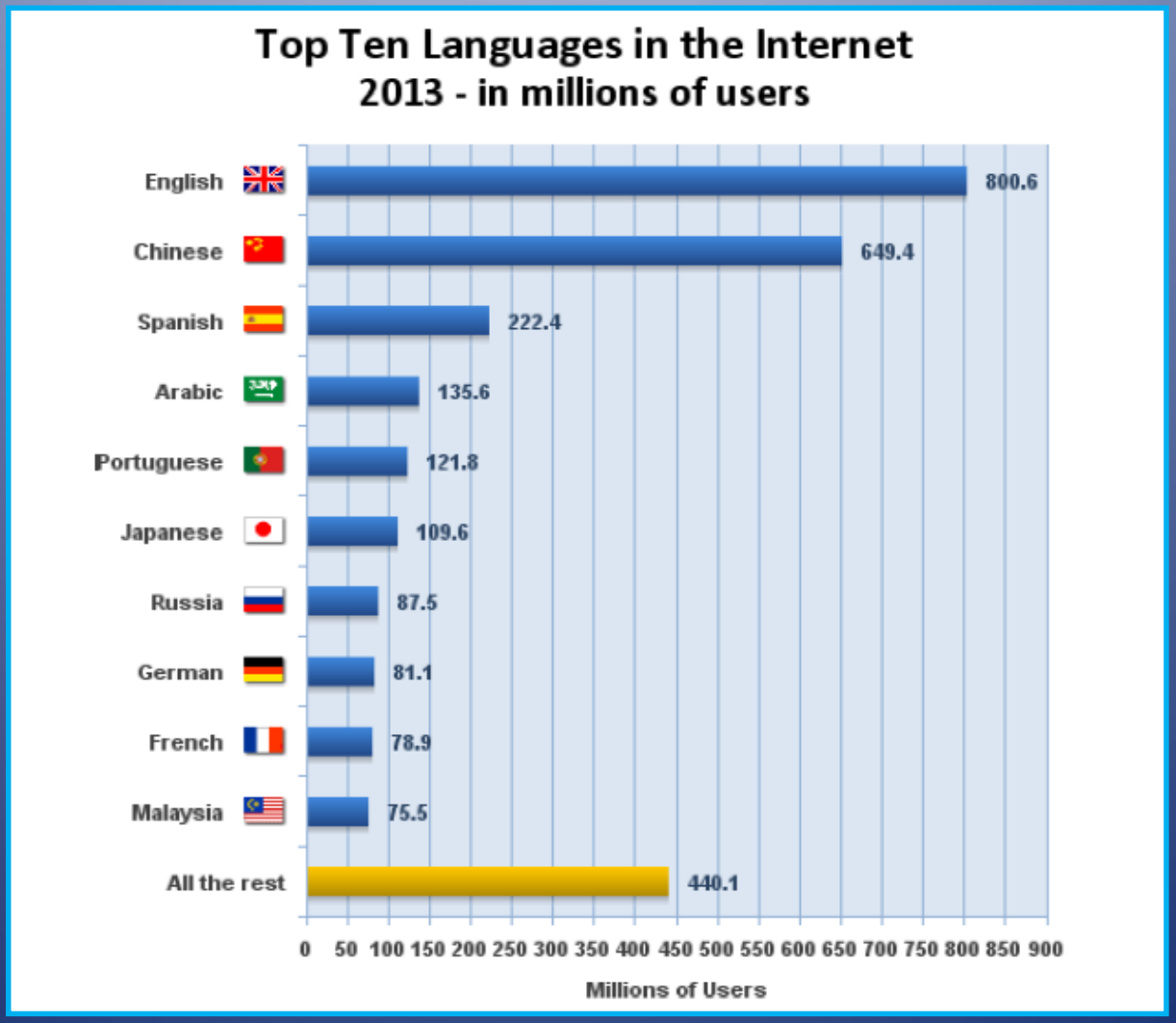
Internet governance should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users.

חופש הביטוי והעברת המידע מעבר לגבולות ריבוניות

- Everyone has the right to freedom of opinion and expression; this right includes freedom to …seek, receive and impart information and ideas through any media and regardless of frontiers. [UD19]

- Interference to electromagnetic communications is prohibited [ITU 45, RR 1]

משילות באינטרנט – אתגר רגולטורי עולמי



World Conference on Int'l Telecommunications (WCIT)-12

OP-ED CONTRIBUTOR

Keep the Internet Open

The decisions taken in Dubai in December have the potential to put government handcuffs on the Net.

- Vinton Cerf

Daniel Haskett

By VINTON CERF
Published: May 24, 2012

The Internet stands at a crossroads. Built from the bottom up, powered by the people, it has become a powerful economic engine and a positive social force. But its success has generated a worrying backlash. Around the world, repressive regimes are putting in place or proposing measures that restrict free expression and affect fundamental rights. The number of governments that censor Internet content has grown to 40 today from about four in 2002. And this number is still growing, threatening to take away the Internet as you and I have known it.

FACEBOOK
TWITTER
GOOGLE+
E-MAIL
SHARE
PRINT
REPRINTS

What's Popular Now

Killing in Greenwich Village Looks Like Hate Crime, Police Say

MOST E-MAILED

1. Criticism of Ve… Mounts Over B…

2. Dagestan's Bitt… by 'Many Tsarr…

3. MOTHERLODE
Ending the Sec… Addiction

4. Spare Times fo…

5. MOTHERLODE
A Solo Trip Tak…

6. THE BOSS
A Life-Changin…

7. Lawmakers Sho… Google's New G…


PROTECT GLOBAL INTERNET FREEDOM
On December 3rd, the world's governments will meet to update a key treaty of a UN agency called the International Telecommunication Union (ITU). Some governments are proposing to extend ITU authority to Internet governance in ways that could threaten Internet openness and innovation, increase access costs, and erode human rights online. We call on civil society organizations and citizens of all nations to sign the following Statement to Protect Global Internet Freedom:
Internet governance decisions should be made in a transparent manner with genuine multistakeholder participation from civil society, governments, and the private sector. We call on the ITU and its member states to embrace transparency and reject any proposals that might expand ITU authority to areas of Internet governance that threaten the exercise of human rights online.

ARTICLE 3A

Internet

(collaborative approach)

31A 3A.1 Internet governance shall be effected through the development and application by governments, the private sector and civil society of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the Internet.

(management of Identification resources)

31B 3A.2 Member States shall have equal rights to manage the Internet, including in regard to the allotment, assignment and reclamation of Internet numbering, naming, addressing and identification resources and to support for the operation and development of basic Internet infrastructure.

(local regulation)

31C 3A.3 Member States shall have the sovereign right to establish and implement public policy, including international policy, on matters of Internet governance, and to regulate the national Internet segment, as well as the activities within their territory of operating agencies providing Internet access or carrying Internet traffic.

(policy on use and operation)

31D 3A.4 Member States should endeavour to establish policies aimed at meeting public requirements with respect to Internet access and use, and at assisting, including through international cooperation, administrations and operating agencies in supporting the operation and development of the Internet.

(protection and security)

31E 3A.5 Member States should ensure that administrations and operating agencies cooperate in ensuring the integrity, reliable operation and security of the national Internet segment, direct relations for the carrying of Internet traffic and the basic Internet infrastructure.

ADD

ARTICLE 3B

Numbering, naming, addressing, and identification resources

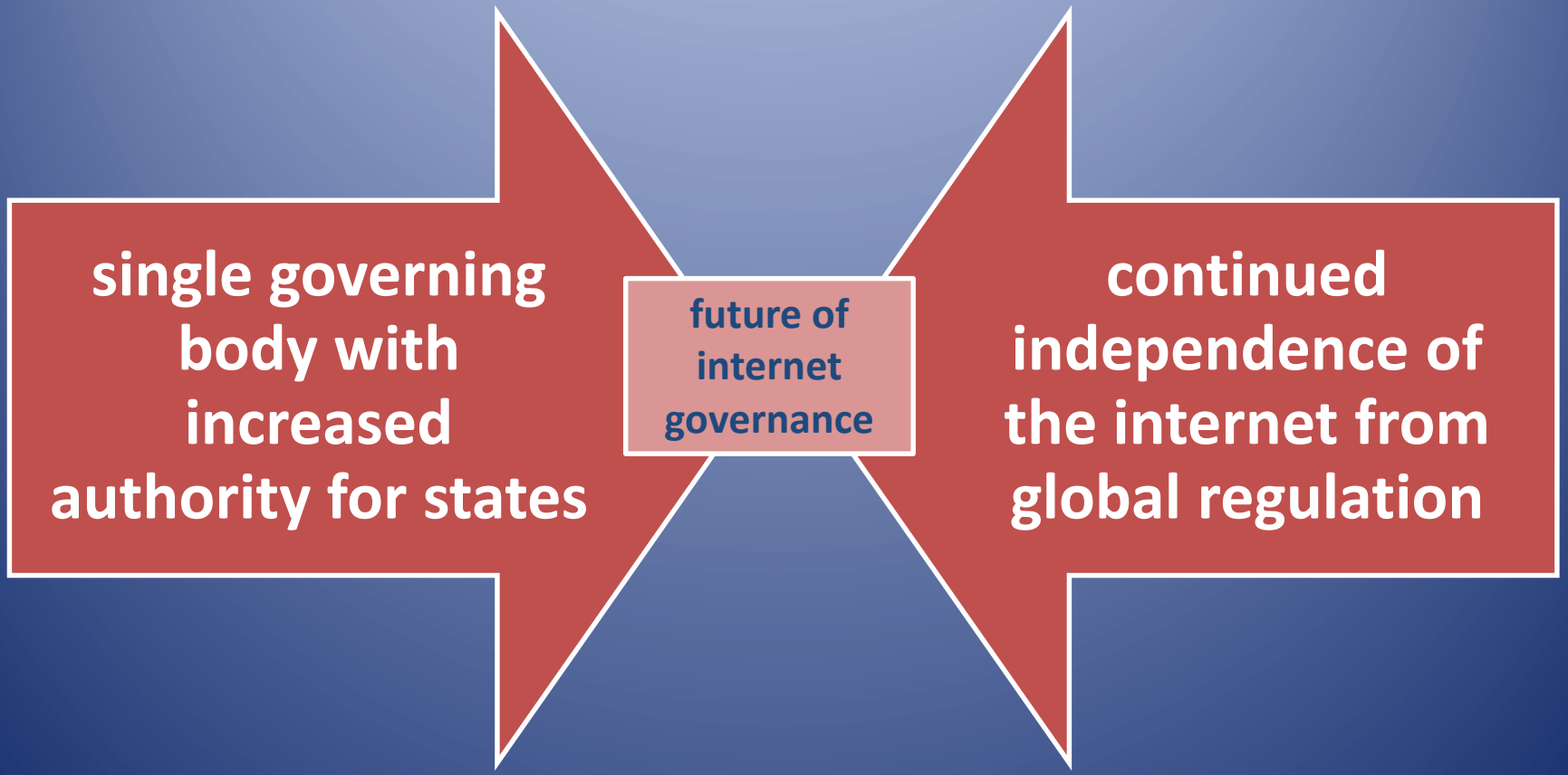
(Fundamental Right)

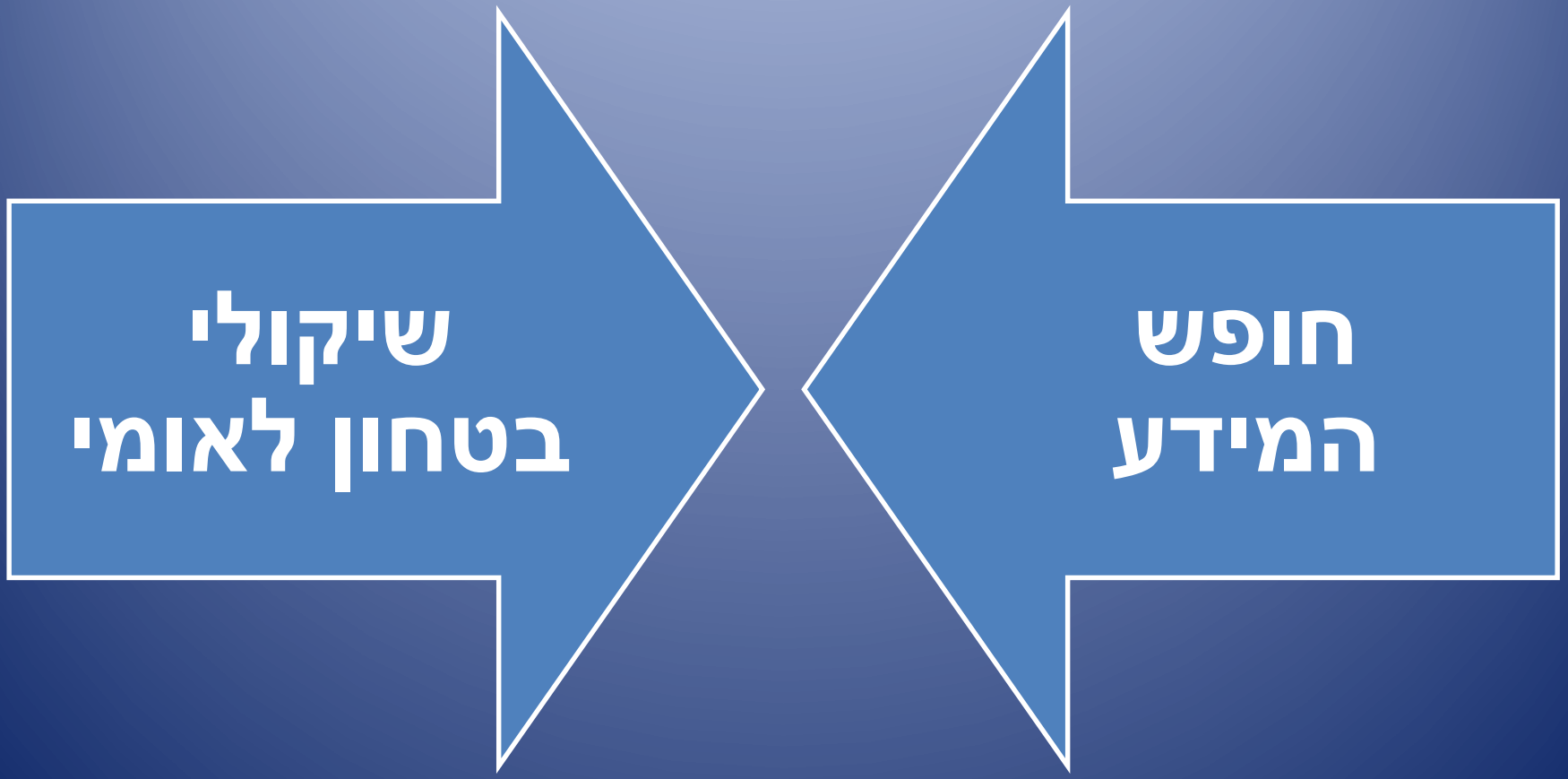
31F 3B.1 Member states have the right to manage all naming, numbering, addressing and identification resources used for international telecommunications/ICT services within their territories.

(Preventing Misuse)

Surprise Article 3A Revision proposed by UAE, Arab states, Russia, China (5/12)

מה בעצם עמד להכרעה ב-WCIT?




חופש
המידע
שיקולי
בטחון לאומי

שיקולים של בטחון לאומי ואזורי

theguardian

NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama . .

Glenn Greenwald

Thursday 6 June 2013 11.05 BST

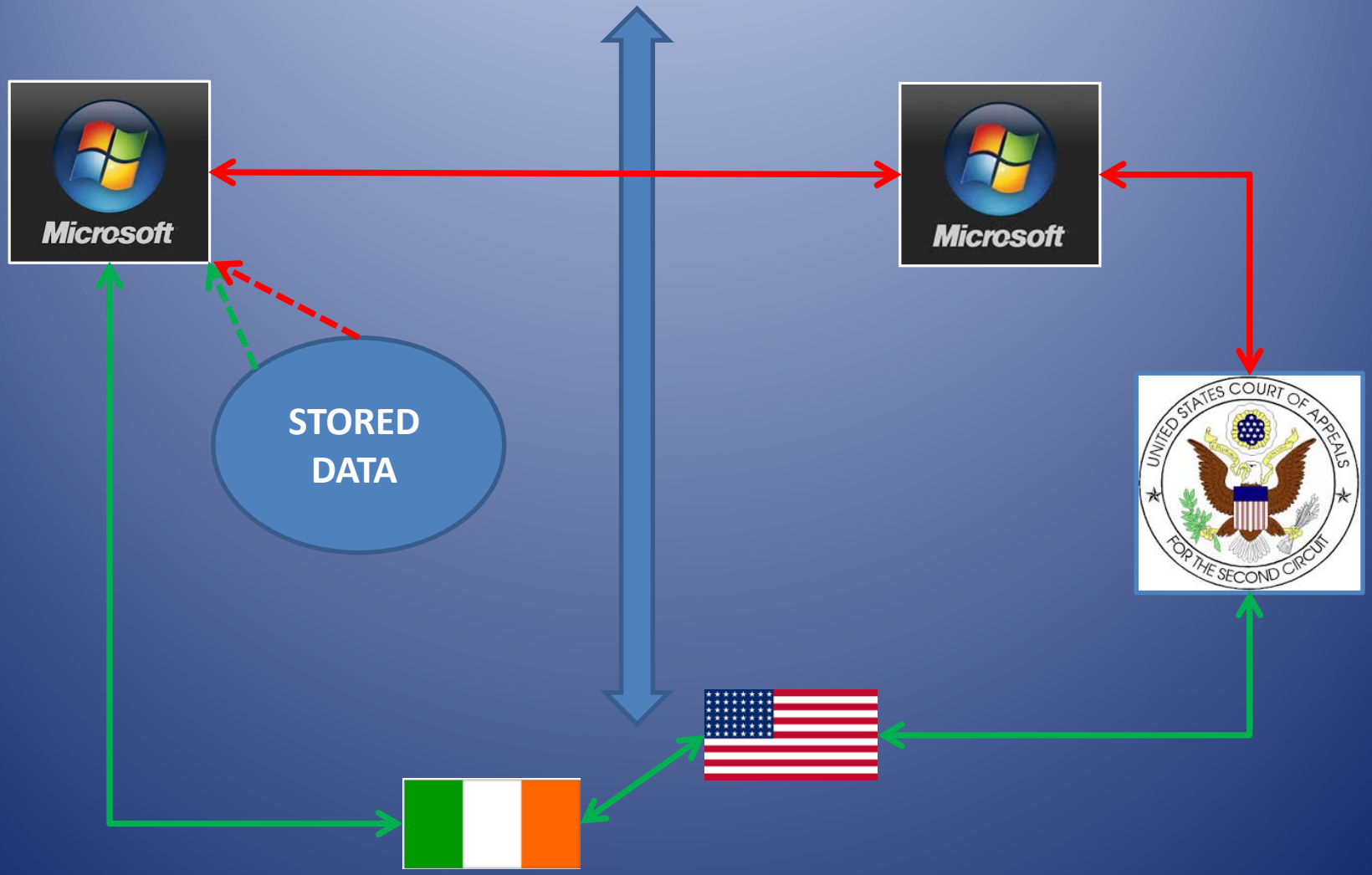
The National Security Agency is currently collecting the telephone records of millions of US customers of Verizon, one of America's largest telecoms providers, under a top secret court order issued in April.

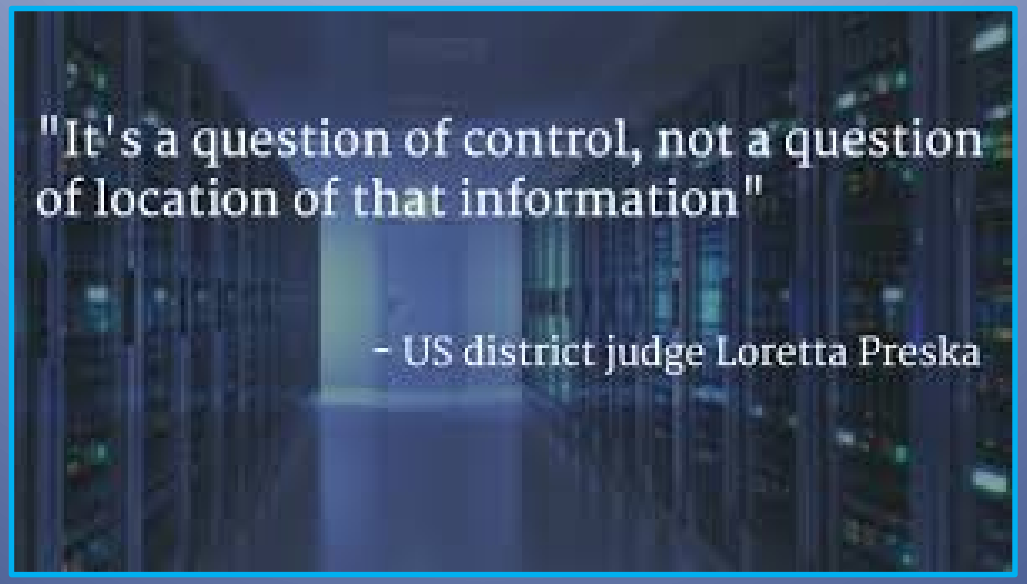
The order, a copy of which has been obtained by the Guardian, requires Verizon on an "ongoing, daily basis" to give the NSA information on all telephone calls in its systems, both within the US and between the US and other countries.

The document shows for the first time that under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk - regardless of whether they are suspected of any wrongdoing.

שיקולים של חופש המידע

האתגר של סמכות שיפוט באינטרנט


Microsoft
Microsoft
STORED
DATA
UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT


"It's a question of control, not a question of location of that information"
- US district judge Loretta Preska

טרור מקוון

Δ's

"טרור מקוון" במדריך טאלין

RULE 36

…. Cyber attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian population….

"מתקפת סייבר"

RULE 30

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.

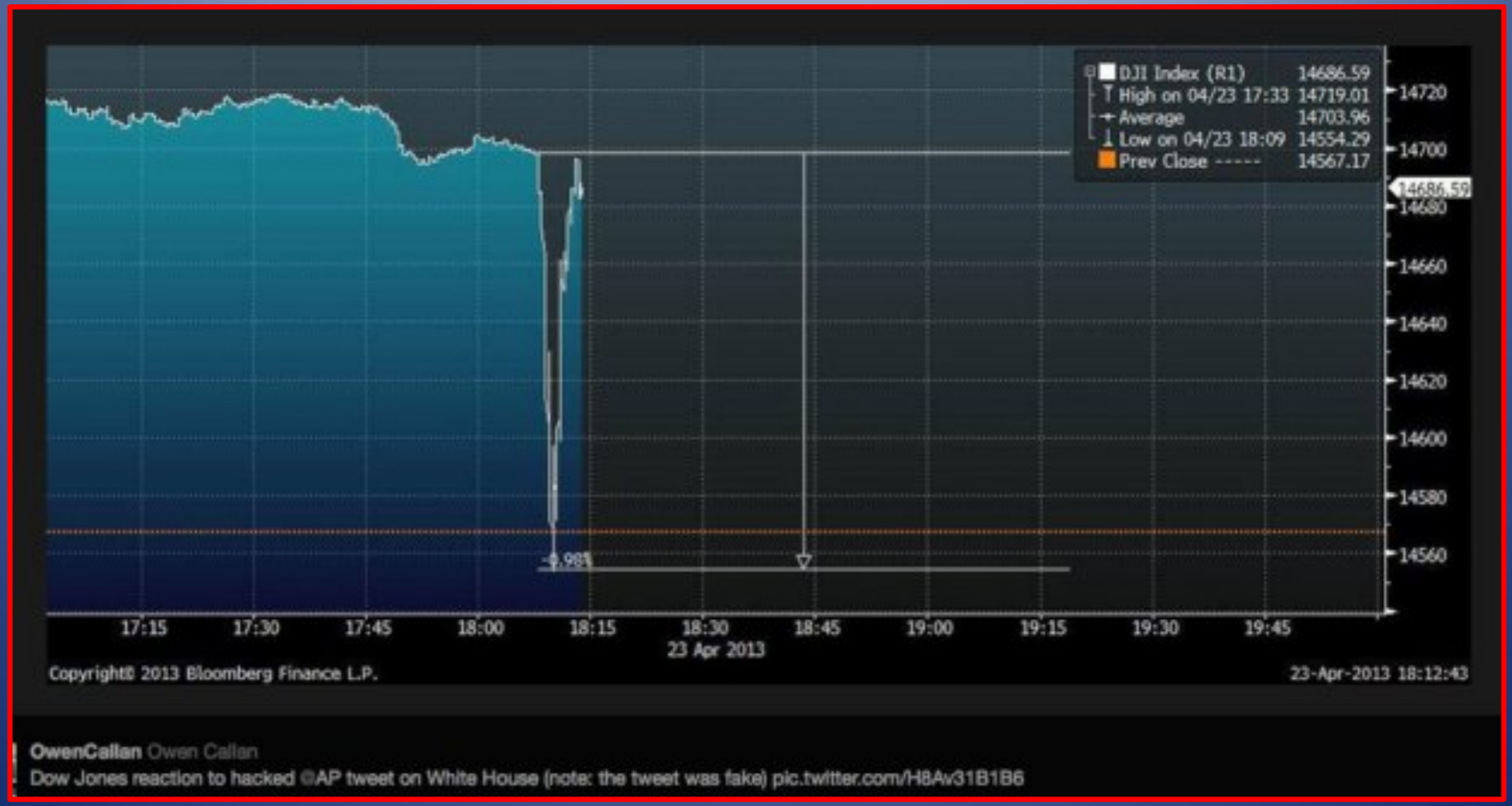
תופעה מתפתחת – חשיבה על ההסדרה

1. • הבחנה בין פעולות תמיכה ופעולות ישירות עם תוצאה בפועל (דוג' עמותות)
2. • יכולות א-סימטריות מוגברות
3. • חשיפה מוגברת של תשתיות קריטיות

מרץ 2013

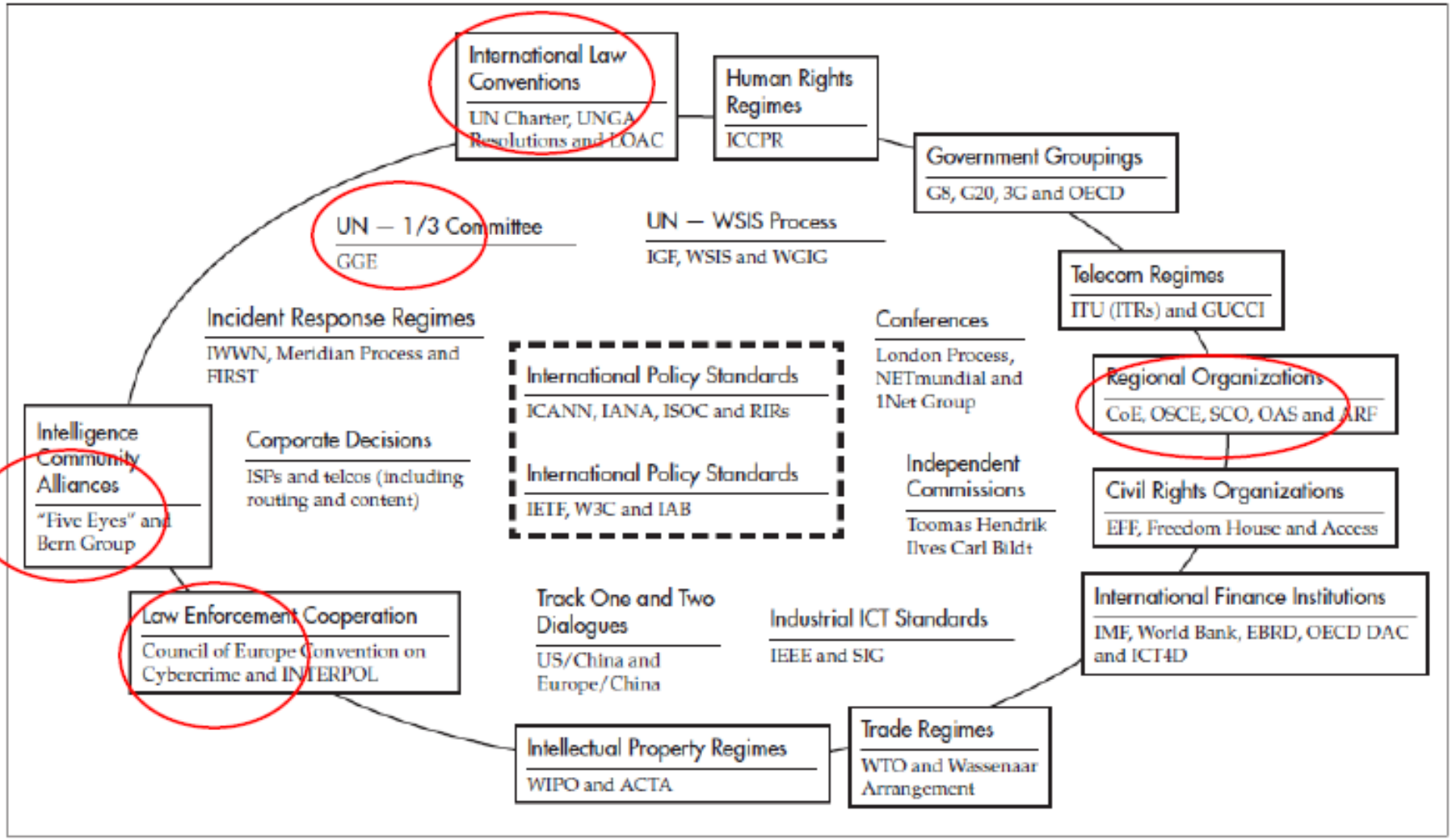

AP
The Associated Press
@AP
Follow
Breaking: Two Explosions in the White House and Barack Obama is injured
Reply
Retweet
Favorite
More
467
RETWEETS
15
FAVORITES
1:07 PM - 23 Apr 13

התוצאה


DJI Index (R1) 14686.59
High on 04/23 17:33 14719.01
Average 14703.96
Low on 04/23 18:09 14554.29
Prev Close ----- 14567.17
14720
14700
14686.59
14680
14660
14640
14620
14600
14580
14560
-0.98%
17:15
17:30
17:45
18:00
18:15
18:30
18:45
19:00
19:15
19:30
19:45
23 Apr 2013
Copyright© 2013 Bloomberg Finance L.P.
23-Apr-2013 18:12:43
OwenCallan Owen Callan
Dow Jones reaction to hacked @AP tweet on White House (note: the tweet was fake) pic.twitter.com/H8Av31B1B6

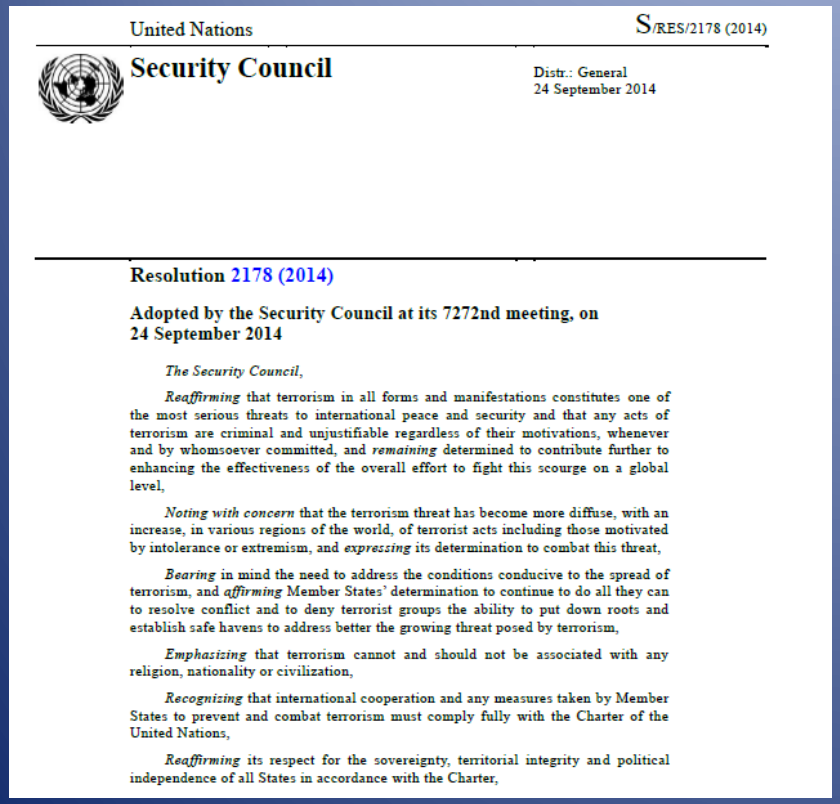
החשיפה הא-סימטרית של תשתיות קריטיות

Figure 1: The Regime Complex for Managing Global Cyber Activities



Source: Author.

UNSC 2178 (2014)



United Nations S/RES/2178 (2014)

Security Council

Distr.: General
24 September 2014

Resolution 2178 (2014)

Adopted by the Security Council at its 7272nd meeting, on 24 September 2014

The Security Council,

Reaffirming that terrorism in all forms and manifestations constitutes one of the most serious threats to international peace and security and that any acts of terrorism are criminal and unjustifiable regardless of their motivations, whenever and by whomsoever committed, and *remaining* determined to contribute further to enhancing the effectiveness of the overall effort to fight this scourge on a global level,

Noting with concern that the terrorism threat has become more diffuse, with an increase, in various regions of the world, of terrorist acts including those motivated by intolerance or extremism, and *expressing* its determination to combat this threat,

Bearing in mind the need to address the conditions conducive to the spread of terrorism, and *affirming* Member States' determination to continue to do all they can to resolve conflict and to deny terrorist groups the ability to put down roots and establish safe havens to address better the growing threat posed by terrorism,

Emphasizing that terrorism cannot and should not be associated with any religion, nationality or civilization,

Recognizing that international cooperation and any measures taken by Member States to prevent and combat terrorism must comply fully with the Charter of the United Nations,

Reaffirming its respect for the sovereignty, territorial integrity and political independence of all States in accordance with the Charter,

Expressing concern over the increased use by terrorists and their supporters of communications technology for the purpose of radicalizing to terrorism, recruiting and inciting others to commit terrorist acts, including through the internet, and financing and facilitating the travel and subsequent activities of foreign terrorist fighters, and underlining the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law,

הגדרת "מעשה טרור" מתוך הצעת החוק המאבק בטרור, 2015

(ג) פגיעה חמורה ברכוש, פגיעה ברכוש שגרמה או שעלולה לגרום לפגיעה חמורה בשלום הציבור או לנזק כלכלי חמור, או פגיעה ברכוש שהיה בה או עלול להיות בה משום פגיעה חמורה במוסדות השלטון;

(ד) פגיעה חמורה בתשתיות, במערכות או בשירותים חיוניים, או שיבוש חמור שלהם, פגיעה חמורה בכלכלת המדינה או בסביבה, או פגיעה בסביבה שגרמה או בסביבה שגרמה או שעלולה לגרום לגרום לנזק כלכלי חמור;

מערכות אכיפה של רגולציית סייבר במישור הבינלאומי

לסיכום

סוגיות בדיני סייבר בינלאומיים: מערכת נורמאטיבית מתפתחת והמוסדות שתומכים בהן

(1) מערכת הבטחון הקולקטיבי במרחב הסייבר

(2) אמנות בינלאומיות

(3) הסדרים איזורים

(4) משילות באינטרנט

(5) טרור מקוון

בין הסוגיות המשפטיות המאתגרות

1. • מי אחראי על ההסדרה מבחינת המוסדות הבינלאומיים והמדינתיים – וכיצד להסדיר?
2. • כיצד מפתחים הגדרות יסוד?
3. • התמודדות עם נושאים מהותיים– ייחוס, שחקנים שאינם מדינות, חופש הביטוי
4. • אכיפת נורמות משפטיות במישור הבינלאומי

תודה רבה.