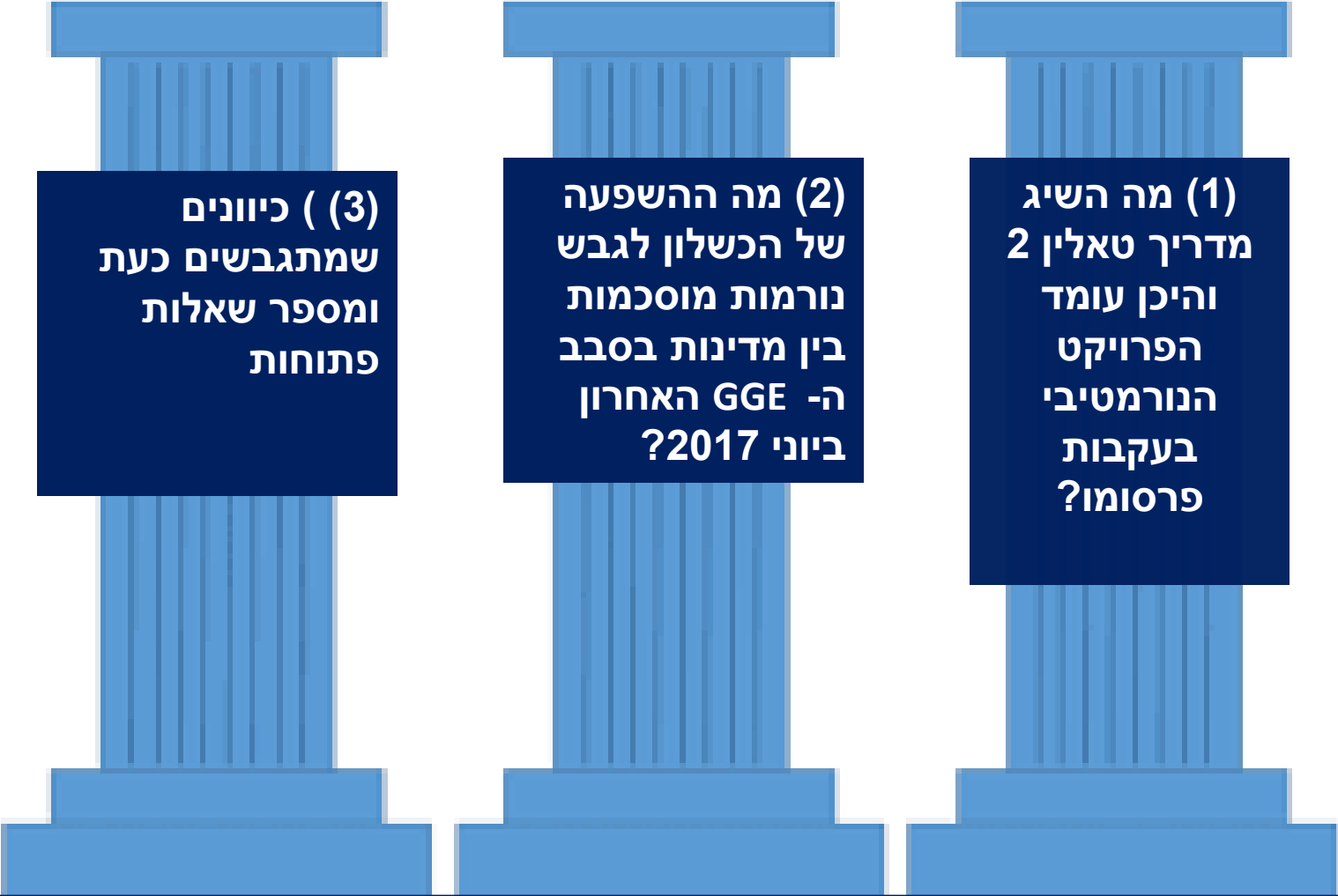


**התפתחויות בדין הבינלאומי שחל על
פעילותם של מדינות וגורמים לא-
מדינתיים במרחב הסייבר: הערכת מצב**

15.11.2017

פורום סייבר של הפקולטה
למשפטים באוניברסיטה
העברית

דב האוסן-כוריאל



(1) מה השיג
מדריך טאלין 2
והיכן עומד
הפרויקט
הנורמטיבי
בעקבות
פרסומו?

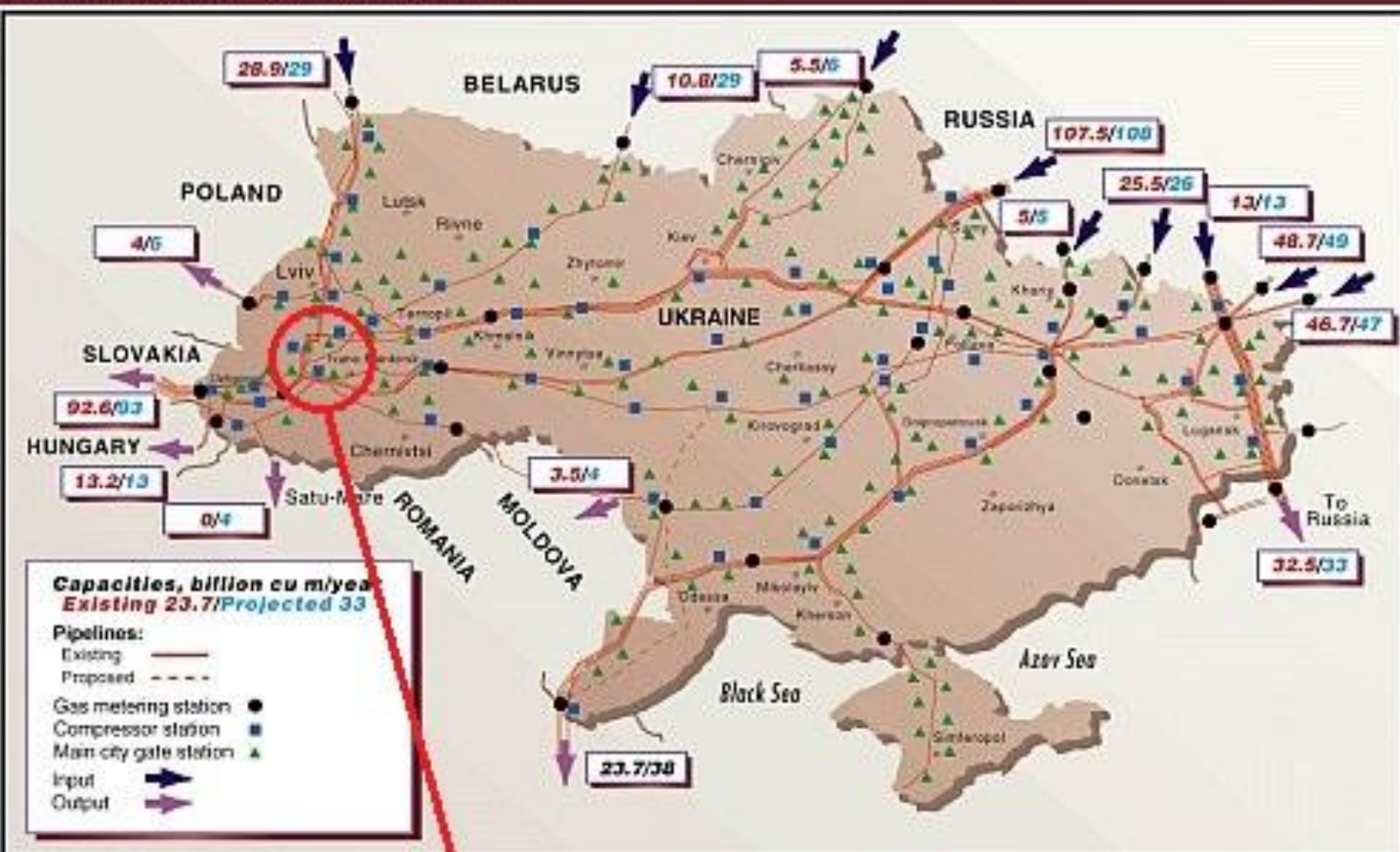
(2) מה ההשפעה
של הכשלון לגבש
נורמות מוסכמות
בין מדינות בסבב
ה- GGE האחרון
ביוני 2017?

(3) כיוונים
שמתגבשים כעת
ומספר שאלות
פתוחות

משבר נורמטיבי מורכב ומעניין



UKRAINE'S GASTRANSMISSION SYSTEM *



*Projected figures are estimates. Map does not show facilities such as underground storage, production, and gas processing plants.

061

Location of power system outage

סוגיית הייחוס

Implications for Defenders

The remote cyber attacks directed against Ukraine's electricity infrastructure were bold and successful. The cyber operation was highly synchronized and the adversary was willing to maliciously operate a SCADA system to cause power outages, followed by destructive attacks to disable SCADA and communications to the field. The destructive element is the first time the world has seen this type of attack against OT systems in a nation's critical infrastructure. This is an escalation from past destructive attacks that impacted general-purpose computers and servers (e.g., Saudi Aramco, RasGas, Sands Casino, and Sony Pictures). Several lines were crossed in the conduct of these attacks as the targets can be described as solely civilian infrastructure. Historic attacks, such as Stuxnet, which included destruction of equipment in the OT environment, could be argued as being surgically targeted against a military target.

דו"ח חוקרי סייבר של E-ISAC בענין פריצת מערכת החשמל במזרח
אוקריינה (במרץ 2016)

- **מקרה תקדימי** – מתקפת סייבר על תשתיות קריטיות אזרחיות

- בהקשר של מלחמה קינטית ("**מלחמה היברידית**")

- **הייחוס** לוקח זמן ואינו תמיד וודאי

- המקרה **חזר על עצמו** בדצמבר 2016; גם גרמניה 2016

- האירוע באוקריינה משאיר אותנו עם מספר שאלות לגבי **הדין החל**

אפילו עם ייחוס
וודאי...

אין מענה בפועל מצד
אוקריינה ואין הכרעות או
הצהרות (פומביות) של
הקהילה הבינלאומית

פשע מקוון-
יחידים /
קבוצה

ענין של
המשכיות
עסקית

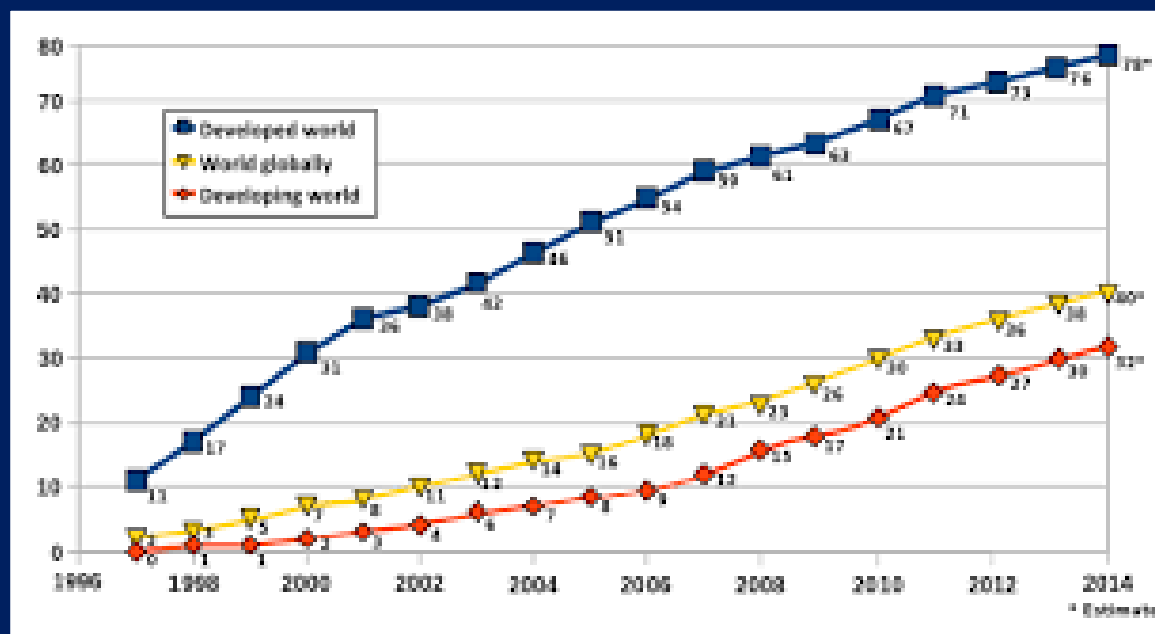
מוש בכוח
שעובר את
הסף של
2(4)

נאט"ו

**מה טיבו של המשבר נורמטיבי כעת – ומה
השלכותיו?**

מציאות חדשה

47% עם
גישה



הגדרות:

החלטת ממשלה 3611, אוגוסט 2011

הגדרות:

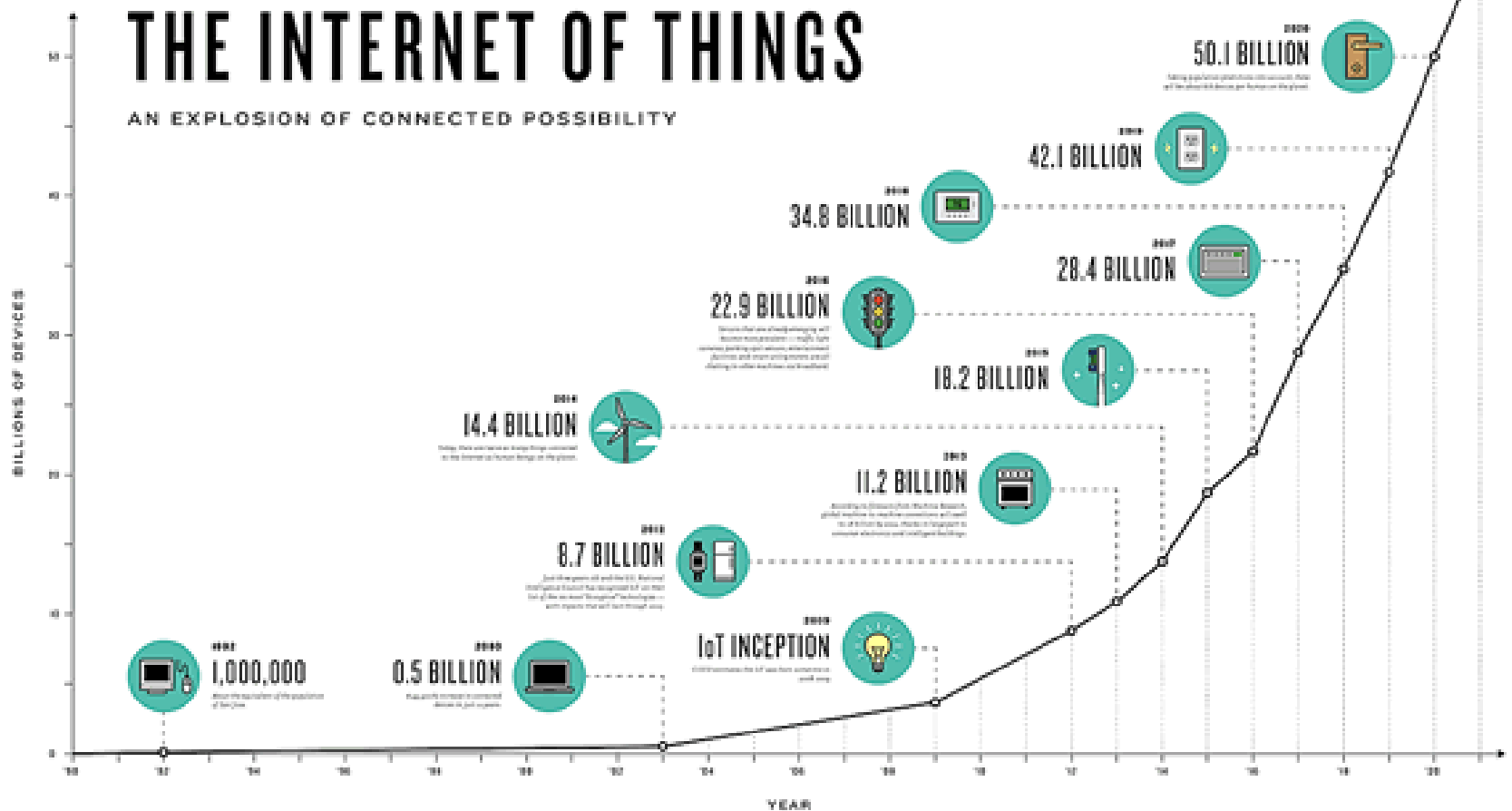
- א. "המרחב הקיברנטי" - המתחם הפיזי והלא פיזי, שנוצר או מורכב מחלק או מכל הגורמים הבאים: מערכות ממוכנות ממוחשבות, רשתות מחשבים ותקשורת, תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה והמשתמשים של כל אלה.
- ב. "ביטחון קיברנטי" - מדיניות, מנגנוני אבטחה, פעולות, הנחיות, ניהול סיכונים וכלים טכנולוגיים, שנועדו להגן על המרחב הקיברנטי ושנועדו לאפשר פעולה בו.

INTERNET OF EVERYTHING

2025

THE INTERNET OF THINGS

AN EXPLOSION OF CONNECTED POSSIBILITY



עלויות קשות במישור הפיננסי, מידע אישי מוגן ובטחון לאומי

Carbanak (2014)
מיליארד \$

NotPetya (2017)
1.2 מיליארד \$

Equifax (2017)
245 מיליון
חשבונות בארה"ב

Yahoo (2014) 5
מיליון חשבונות

NSA

Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core

A serial leak of the agency's cyberweapons has damaged morale, slowed intelligence operations and resulted in hacking attacks on businesses and civilians worldwide.

By SCOTT SHANE, NICOLE PERLROTH and DAVID E. SANGER NOV. 12, 2017

Fifteen months into a wide-ranging investigation by the agency's counterintelligence arm, known as Q Group, and the F.B.I., officials still do not know whether the N.S.A. is the victim of a brilliantly executed hack, with Russia as the most likely perpetrator, an insider's leak, or both. Three employees have been arrested since 2015 for taking classified files, but there is fear that one or more leakers may still be in place. And there is broad agreement that the damage from the Shadow Brokers already far exceeds the harm to American intelligence done by Edward J. Snowden, the former N.S.A. contractor who fled with four laptops of classified material in 2013.

השלכות

- **חוסר-וודאות** לגבי החלת הדין הבינלאומי במרחב הסייבר
 - מהי ייחשב שימוש בכוח במרחב?
 - האם חברה פרטית שסופגת פריצת סייבר יכולה לבצע hackback?
- קושי בהבנת **כוונותיהן של מדינות** במרחב
 - פעילות לא שקופה
- **ריבוי נסיונות לגבש הסדרים** נורמטיביים
 - Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building
 - יוזמות מיקרוסופט

שתי גישות למשבר (2017)

Macak, From Cyber Norms to Cyber Rules: Re-engaging States as Lawmakers

- **מדינות מהססות ליצור נורמות מחייבות** במרחב, כיוון שרוצות לשמר חופש פעולה לעצמן
- בגלל קשיים ביצירת הסכמה נורמטיבית מחייבת במישור הבינלאומי, הן **"בורחות"** ל-CBMs ו-voluntary norms
- ולכן נוצרה **lacuna** אליה נכנסים גורמים **לא-מדינתיים** (מדריך טאלין וחב' מיקרוסופט)
- "International cybersecurity law is at **a critical juncture** today."
- **מדינות חייבות להתחיל לפעול**, כיצרני המשפט הבינלאומי.

Finnemore and Hollis, Constructing Norms for Global Cybersecurity

- **להתמקד בתהליך של יצירת נורמות** מחייבות, ולא רק הנורמה כ"מוצר" (product)
- "[T] the real power of norms... lies in the processes by which they form and evolve. **The success of a norm rests not just in what it says, but in who** accepts it, not to mention **where, when, and how** they do so. It matters to the content and future of a norm, for example, whether it is promulgated by states at the United Nations, technologists in an industry association, privacy activists in a nongovernmental organization (NGO), or some freestanding multistakeholder group open to all these actors."
- נורמות במרחב הסייבר **כבר בהתפתחות** – אבל לא לפי המודל שהכרנו עד כה.
- **המשבר הוא מושגי** (ובעצם – הצעה להתגרש מהמודל המוכר של המשפט הבינלאומי)

הצעה **לגישה שלישית:** להפריד בין התהליך הפרוצדורלי של
גיבוש נורמות במרחב לבין הבירור המהותי

• **פרוצדורלית** – יש בהחלט משבר סביב התהליך
של גיבוש הבנה נורמטיבית

– **אמנה לא תהיה** בקרוב -המצב הגיאופוליטי

– הבדלי גישה לגבי ה"איך"

– מיהם **השחקנים** הלגיטימיים?

• **מהותית** – האתגר אינו מצדיק את הכינוי "משבר"

– **אין ריק:** דיני הבזק הבינלאומיים, הגנת מידע אישי

והגנת IP מתפתחות יפה, גם שימוש בכוח במרחב

שיש לו תוצאה קינטית

- יש קשיים מהותיים שאינם מספיק נוכחים בשיח של קהילת המשפטנים הבינלאומיים

- חלוקת המשימה הנורמטיבית תאפשר להתמקד בהם

- הגנה עצמית והגנה עצמית מקדימה במרחב (פס ייצור של שירותים ומוצרים)

- העדר הפרדה בין "המרחב הצבאי" ל-"מרחב האזרחי"

- מהו מידע?

- נשק, נכס, חלק מהזהות שלנו, שירות, קשר (relationship)

- יש כעת תפקיד קריטי למחקר אקדמי ובירורי track

- 2 – מדינות עדיין לא מוכנות לחשוף עמדות

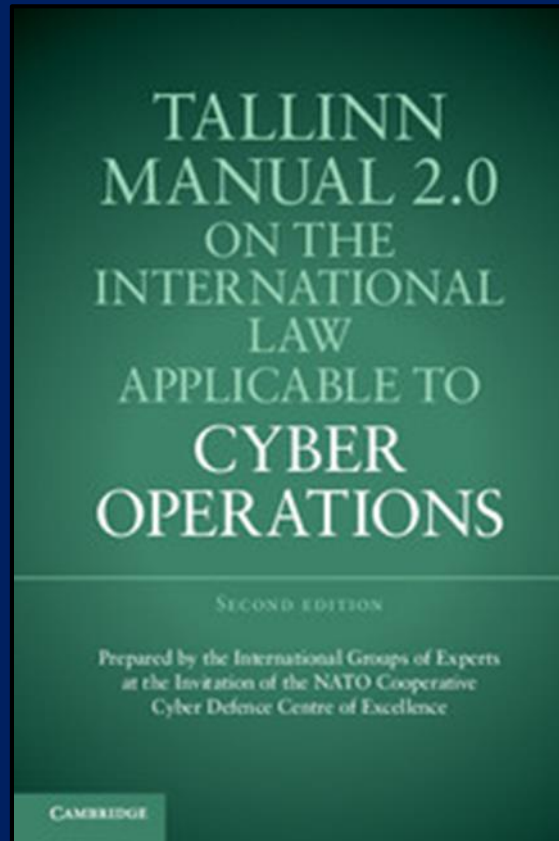
ההפרדה בין פרוצדורה למהות
קריטית כדי להתקדם בצורה מושכלת

יתכן **תהליך ביניים** של CBMs, נורמות
רכות כדי לטפל בבעיות המיידיות
--- חשיפה של תשתיות קריטיות

ההפרדה האמורה
כבר מתחילה בין
מדינות במערב-
GCSC

**(1) מה השיג מדריך טאלין 2 והיכן עומד הפרויקט
הנורמטיבי בעקבות פרסומו?**

מדריך טאלין 1 + 2



ריבונות וסמכות השיפוט של מדינות במרחב

Rule 1 -The principle of State sovereignty applies in cyberspace.

Rule 2 – A State enjoys sovereign authority with regard to the cyber infrastructure, persons and cyber activities located within its territory, subject to its international legal obligations.

- Cyber infrastructure: The communications, storage and computing devices upon which information systems are built and operate.

Rule 4 - Violation of sovereignty

A State must not conduct cyber operations that violate the sovereignty of another State.

Rule 6 – Due diligence

A State must exercise due diligence in not allowing its territory...to be used for cyber operations that affect the rights of other States.

סמכות שיפוט

Rule 8 – Jurisdiction (general principle)

Subject to limitations set forth in international law, a State may exercise territorial and extraterritorial jurisdiction over cyber activities.

- Territorial jurisdiction over cyber infrastructure and persons engaged in cyber activity on its territory
- Cyber activities originating in or completed on its territory
- Cyber activities having a substantial effect on its territory

Rule 61 – Duty to establish, maintain, and safeguard international telecommunication infrastructure

A State must take measures to ensure the establishment of international telecommunication infrastructure that is required for rapid and uninterrupted international telecommunications. If, in complying with this requirement, the State establishes cyber infrastructure for international telecommunications, it must maintain and safeguard that infrastructure.

הגדרת "שימוש בכוח" - Rule 69

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)

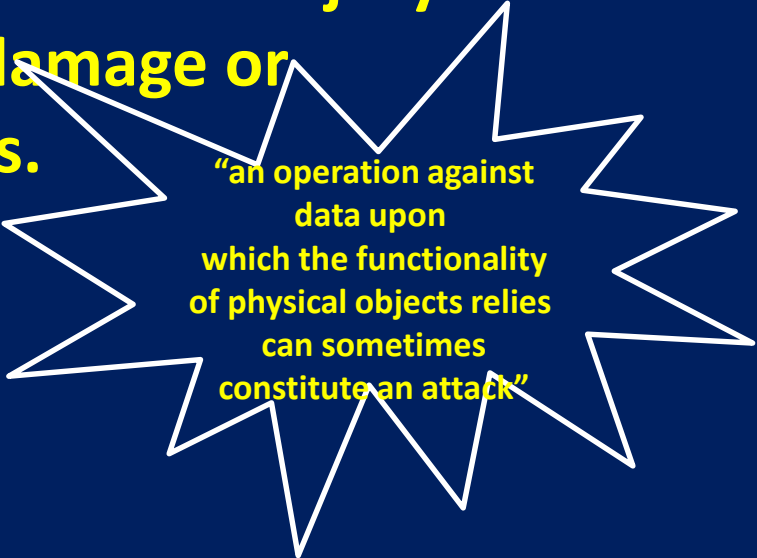
הגנה עצמית – Rule 71

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)

Rule 92- "מתקפת סייבר"

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.**



"an operation against data upon which the functionality of physical objects relies can sometimes constitute an attack"

באותן השנים בהן מתגבש מדריך טאלין 2

הצהרות חד-צדדיות של מדינות וארגונים
בינלאומיים



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

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.

הפרלמנט ההולנדי, 2012

An organised cyber attack on essential state functions must be regarded as an 'armed attack' within the meaning of article 51 of the UN Charter if it causes (or has the potential to cause) serious disruption to the functioning of the state or serious or prolonged consequences for the stability of the state, even if there is no physical damage or injury. In such cases, there must be a disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks...

Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General

[Original: Chinese and Russian]

International code of conduct for information security

Each State voluntarily subscribing to this Code of Conduct pledges:

(1) To comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries;

(2) Not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security;

(3) Not to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability;

(4) To cooperate in combating criminal and terrorist activities that use information and communications technologies and information and communications networks, and in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds;

(2) מה היה הכשלון לגביש נורמות מוסכמות בין GAO האחרון ביוני 2017?

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

VI. How international law

24. The 2013 report stated that international law, as reflected in the United Nations Charter, is applicable and is a framework for the use of ICTs and promoting an open, secure, stable, accessible and peaceful ICT environment. Pursuant to its mandate, the present Group considers the application of international law to the use of ICTs by States.

25. The adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment. These obligations are central to the examination of the application of international law to the use of ICTs by States.

26. In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining 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; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.

27. State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.

The UN GGE is dead: Time to fall forward

Commentary

Stefan Soesanto & Fosca

D'Incau

15th August, 2017

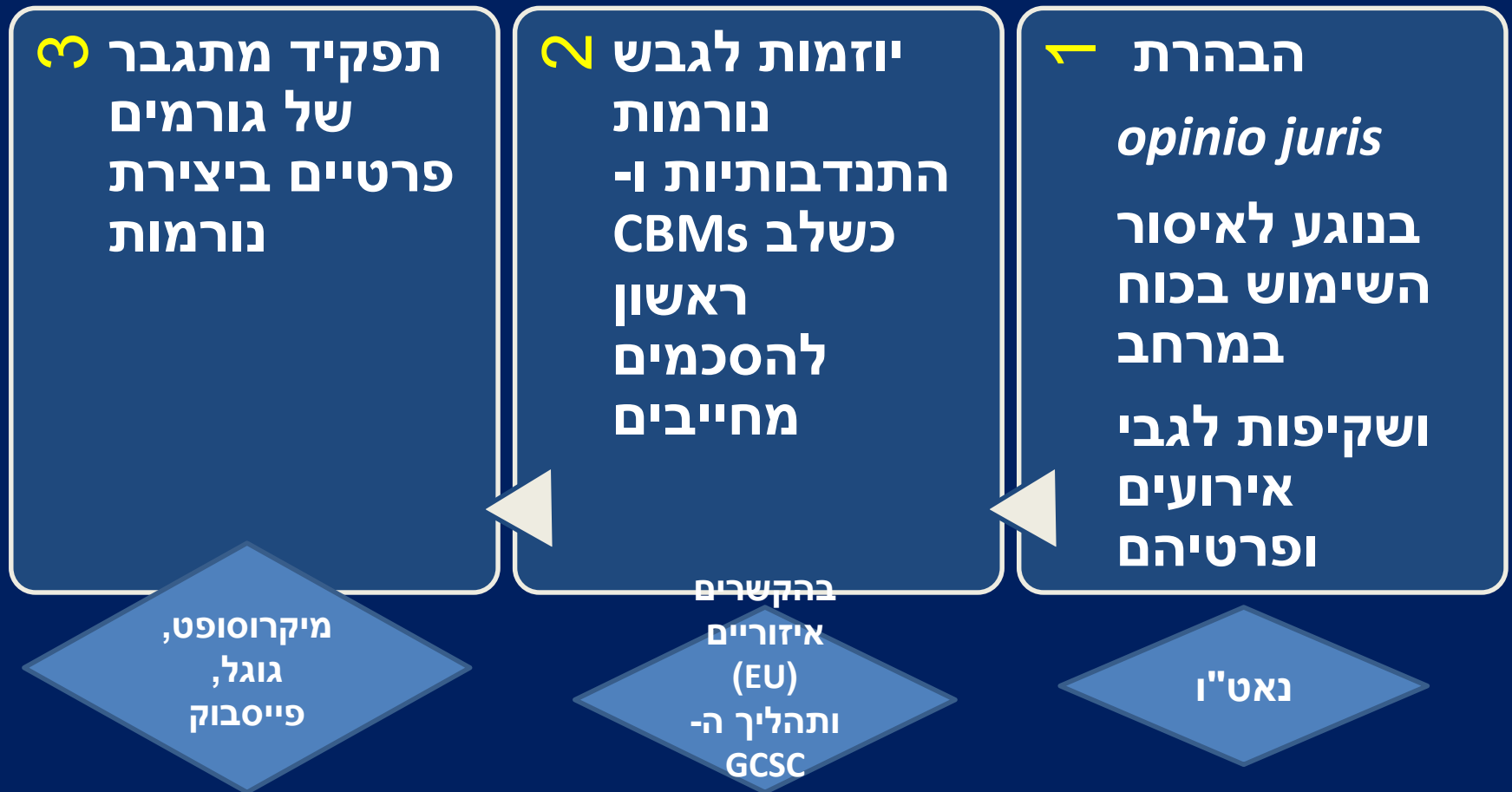
The top down UN GGE process appears dead in the water. International norms and laws for responding to cyber attacks must now be built from the bottom up.

Rules must be binding, violations must be punished, and words must mean something. The UN GGE failed on all three accounts.



מכאן תחושת
המשבר

(3) כיוונים שמתגבשים כעת ומספר שאלות פתוחות



KEY #	OPERATIVE MEASURE	Number of initiatives incorporating the measure (out of 84)
4.1	Information sharing measures in general (information about strategies, policies, legislation, best practices, capacity building)	43
19	Mechanisms for international cooperation (conferences, task forces, cyber diplomacy, learning exchanges, dedicated websites)	35
9	Mechanisms for government - private sector cooperation	31
5.3	Specific mechanisms for transnational law enforcement cooperation and mutual legal assistance for cybercrime	30
4.2	Establishment of a specific national or organizational point of contact for information exchange (including mandate or suggestion of CERT, CSIRT specifically)	29
6	Technical standards recommended or required	27
15	Creating a culture of cybersecurity or information security	25
4.6	"Regular dialogue"	23
4.3	Threat sharing (in general)	23
10	Mechanisms for government - third sector cooperation (NGO's, academia, civil society, informal groups)	22
3	Developing common terminology	21
8.2	Mechanisms for protecting critical infrastructure and essential services	19
4.4	Real-time, 24/7 exchange	18
18	Closing the digital divide	15
14	Cyber education programs	14
12	Supply chain supervision	13

4.5	Mechanisms should be established for communicating vulnerability disclosures	10
23	Publication of statistics, metrics and indicators mandated or recommended	10
11	Mechanisms for B2B cooperation	9
13	Development, training and certification of cybersecurity personnel	9
17	Conducting cyber simulation exercises and tabletops	9
8.1	Common CI (critical infrastructure) terminology	8
22	Development of risk assessment mechanisms for increasing cybersecurity, including insurance risk assessment	7
24	Ensuring technical interoperability of networks	7
7	Certification of professionals, products or services recommended or required	7
1	Specification of government institutions or entities responsible for cyber governance	6
4.7	Information Sharing and Analysis Centers (ISACs) mandated or suggested	6
21	Security / privacy by design for products, systems and services is recommended	6
5.5	Programs to educate and train national legislators and other legal/regulatory personnel on cybersecurity	6
27	Promotion of gender, youth and other diversity cyberspace workforce / engagement	5
5.2	Common definitions of cybercrimes	5
26	Promotion of e-governance	3
4.9	Cyber hotline for issues that may escalate	5

5.4	Mechanism for attribution of hostile cyber activities	2
16	Developing cybersecurity leadership	2
25	Utilize generic identity certificates (digital certification) for user authentication	2
4.8	FIRSTs mandated or suggested	1

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



An attribution organization to strengthen trust online

Microsoft Policy Papers



Establishing an **International Cyberattack Attribution Organization** to strengthen trust online

Today's digital world depends on people, businesses and governments trusting in technology and in the systems that protect them. If someone steals or damages physical property, investigators can collect evidence and involve the courts. In the digital world, the evidence of cyberattacks is often spread across technology providers, telecom operators, and victims. That evidence can also be highly technical, with only a limited number of experts in either the public or private sectors that can find it and analyze it. Furthermore, if it is a government behind the cyberattack then the challenge of proving their responsibility becomes all the more complex.

The world needs a new form of cyber defense. **An organization that could receive and analyze the evidence related to a suspected state-backed cyberattack, and that could then credibly and publicly identify perpetrators, would make a major difference to the trust in the digital world.** It would also give governments a legitimate basis to take further action against the perpetrators. **The technology sector should work with supportive non-profit groups, to create such an organization and help deter nation state attacks in cyberspace.**



נקודת תפנית כפולה: בירור נורמות וגיבוש תהליך מתאים

משבר נורמטיבי מורכב ומעניין

– הגנה עצמית והגנה עצמית מקדימה במרחב (פס ייצור של שירותים ומוצרים)

– העדר הפרדה בין "המרחב הצבאי" ל-"מרחב האזרחי"

– מהו מידע?

• נשק, נכס, חלק מהזהות שלנו, שירות, קשר (relationship)

תודה רבה.

US officially accuses Russia of hacking DNC and interfering with election

Administration says 'only Russia's senior-most officials' could have signed off on cyber-attacks and urges states to seek federal security aid for voting systems

Spencer Ackerman and Sam Thielman in New York

Saturday 8 October 2016 14.09 BST

The US government has formally accused Russia of hacking the Democratic party's computer networks and said that Moscow was attempting to "interfere" with the US presidential election.

Hillary Clinton and US officials have blamed Russian hackers for stealing more than 19,000 emails from Democratic party officials, but Friday's announcement marked the first time that the Obama administration has pointed the finger at Moscow.

"We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities," said the office of the director of national intelligence and the Department of Homeland Security (DHS) in a joint statement.

The accusation marked a new escalation of tensions with Russia and came shortly after the US secretary of state, John Kerry, called for Russia to be investigated for war crimes in Syria.

Vladimir Putin's spokesman dismissed the accusation as "rubbish."



Virus discovered at the Gundremmingen nuclear plant in Germany

April 26, 2016 By Pierluigi Paganini

f My Page

Like 62



According to the German BR24 News Agency, a computer virus was discovered in a system at the Gundremmingen nuclear plant in Germany.

According to the German BR24 News Agency, a computer virus was discovered at the Gundremmingen nuclear power plant in Germany.

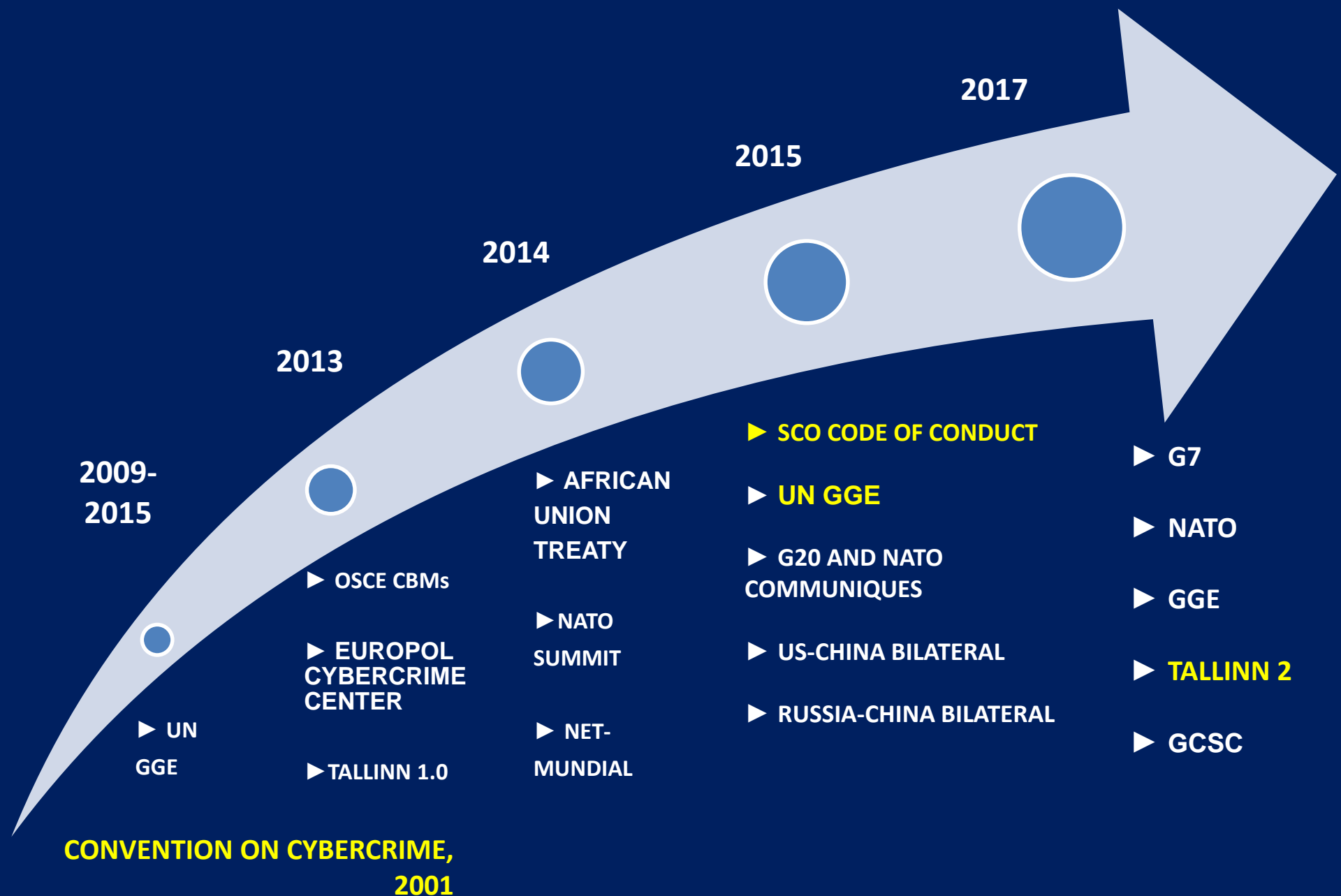
G7 DECLARATION ON RESPONSIBLE STATES BEHAVIOR IN CYBERSPACE

LUCCA, 11 APRIL 2017

We reaffirm and note with approval the widespread affirmation by other States that international law and, in particular, the United Nations Charter is applicable to the use of ICTs by States. This affirmation is essential to maintaining peace and security and promoting an open, secure, stable, accessible and peaceful ICT environment;

We also reaffirm that the same rights that people have offline must also be protected online and reaffirm the applicability of international human rights law in cyberspace, including the UN Charter, customary international law and relevant treaties;

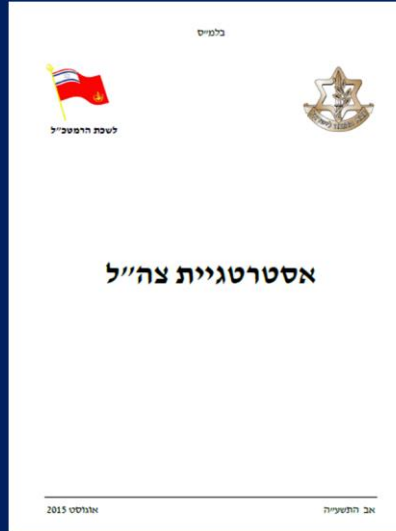
We reiterate the responsibility of States to refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations;



**“THE US MILITARY MAY CONDUCT CYBER OPERATIONS
TO COUNTER AN IMMINENT OR ON-GOING ATTACK
AGAINST...US INTERESTS IN CYBERSPACE. THE
PURPOSE OF SUCH A DEFENSIVE MEASURE IS TO
BLUNT AN ATTACK AND PREVENT THE DESTRUCTION
OF PROPERTY OR THE LOSS OF LIFE.”**



DOD, 2015



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

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