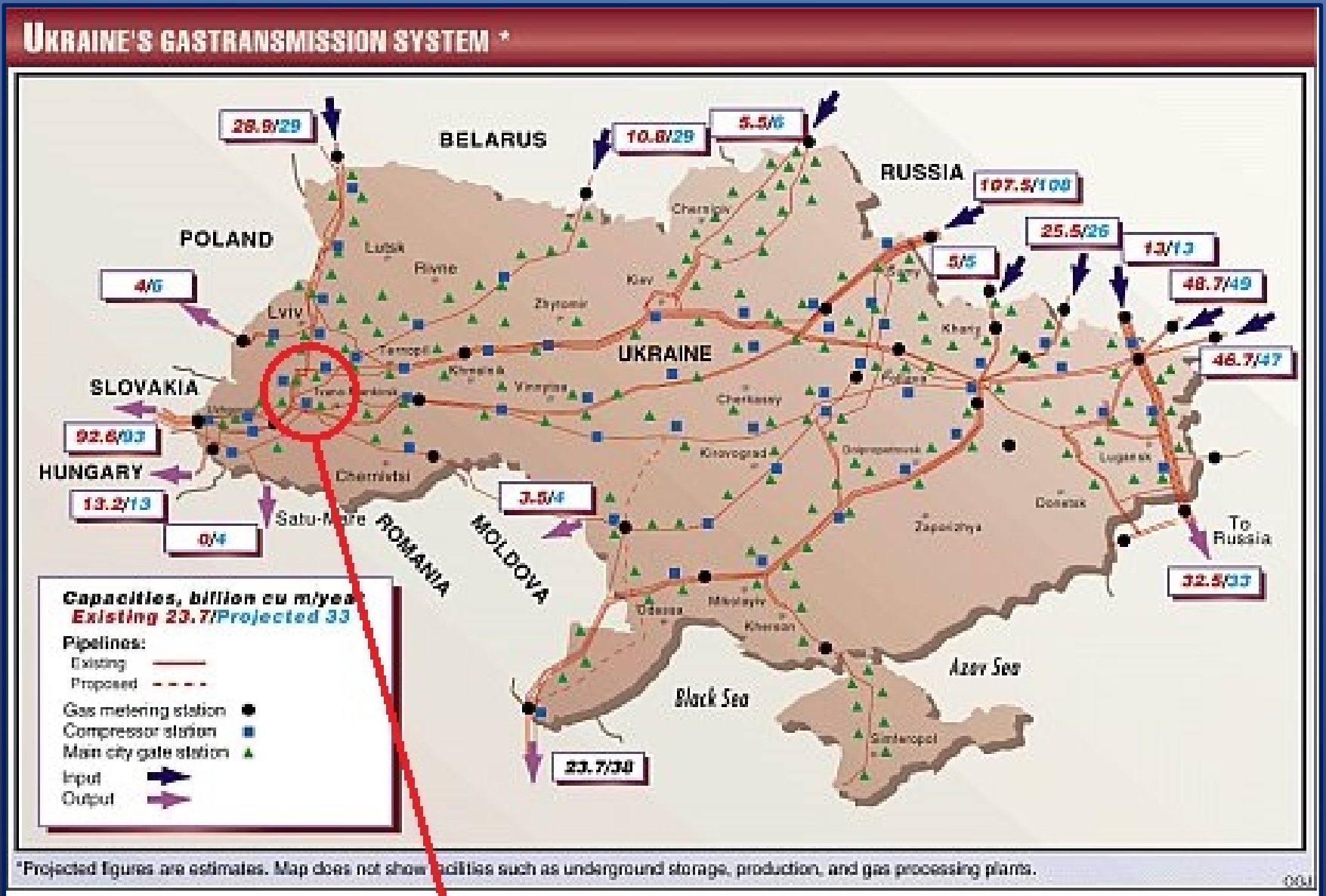
INTERNATIONAL PERSPECTIVES ON CYBERSECURITY: THRESHOLDS OF ENGAGEMENT

DEBORAH HOUSEN-COURIEL, ADV.

FACULTY OF LAW, UNIVERSITY OF HAIFA
TEL AVIV UNIVERSITY INTERDISCPLINARY CYBER RESEARCH CENTER



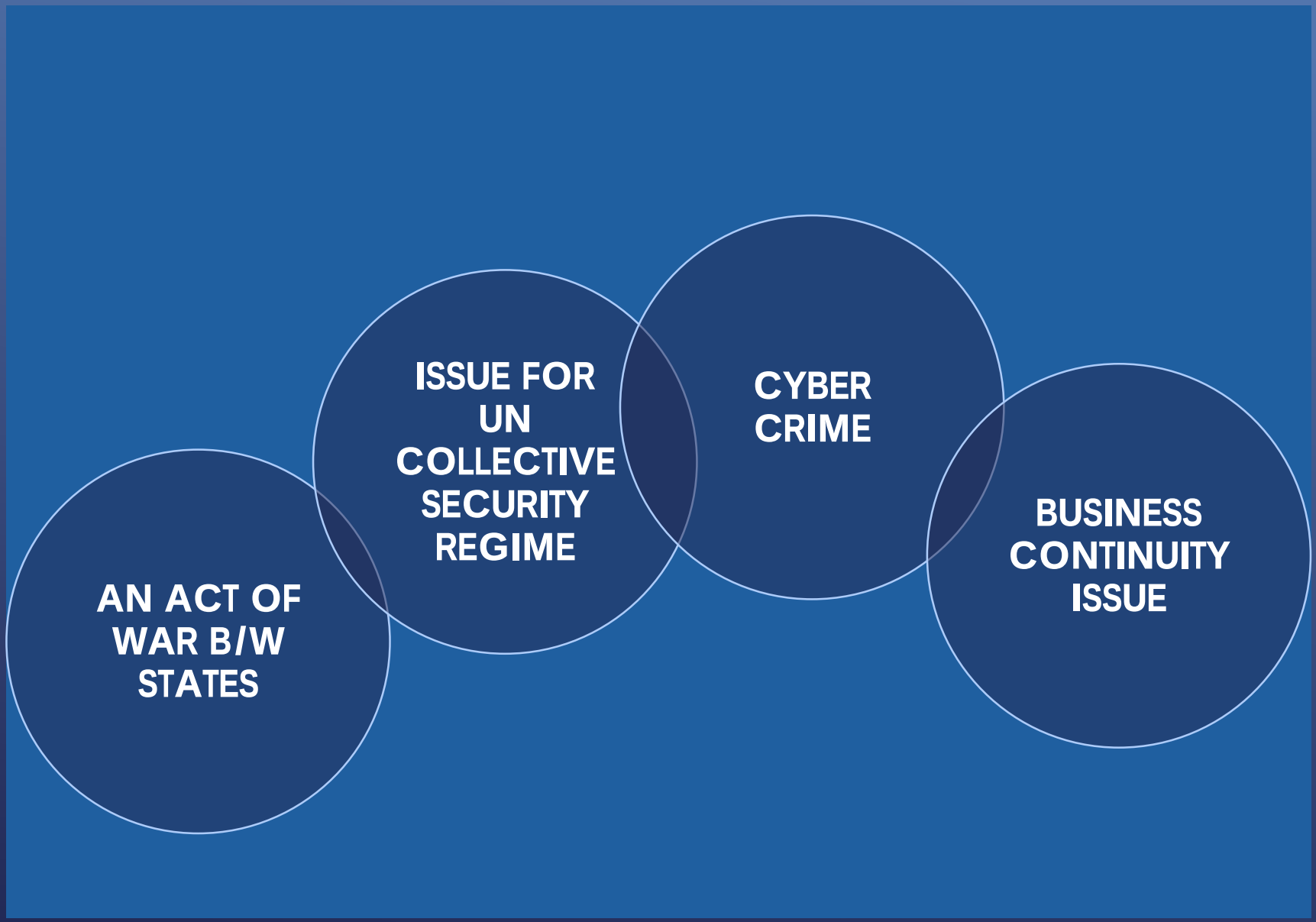
Location of power system outage

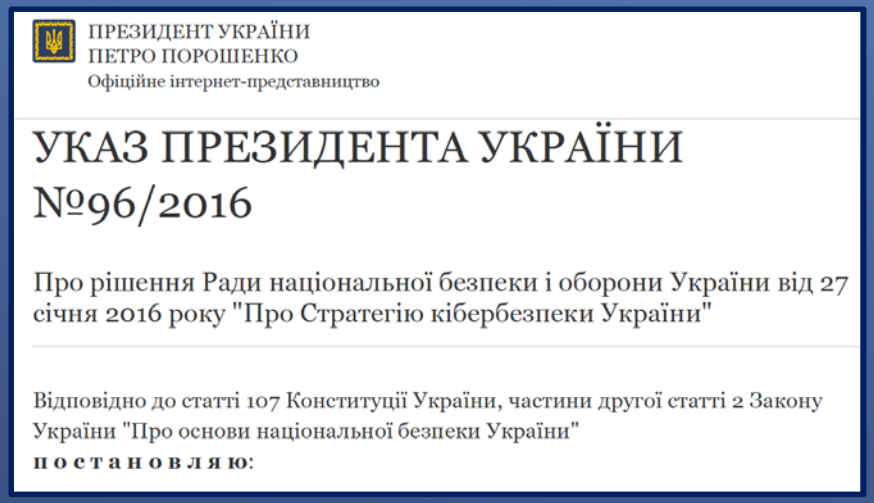
Implications for Defenders

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.

E-ISAC ANALYSIS OF THE CYBER ATTACK ON THE UKRAINIAN POWER GRID, March 2016

- UNPRECEDENTED
- “KINETIC WAR” CONTEXT
- FORMALLY UNATTRIBUTED – RUSSIA?
- NO KNOWN UKRAINIAN RESPONSE – GERMANY TOO
- LEAVES US WITH NOW-FAMILIAR OPEN QUESTIONS….


AN ACT OF WAR B/W STATES
ISSUE FOR UN COLLECTIVE SECURITY REGIME
CYBER CRIME
BUSINESS CONTINUITY ISSUE



ПРЕЗИДЕНТ УКРАЇНИ
ПЕТРО ПОРОШЕНКО
Офіційне інтернет-представництво

УКАЗ ПРЕЗИДЕНТА УКРАЇНИ
№96/2016

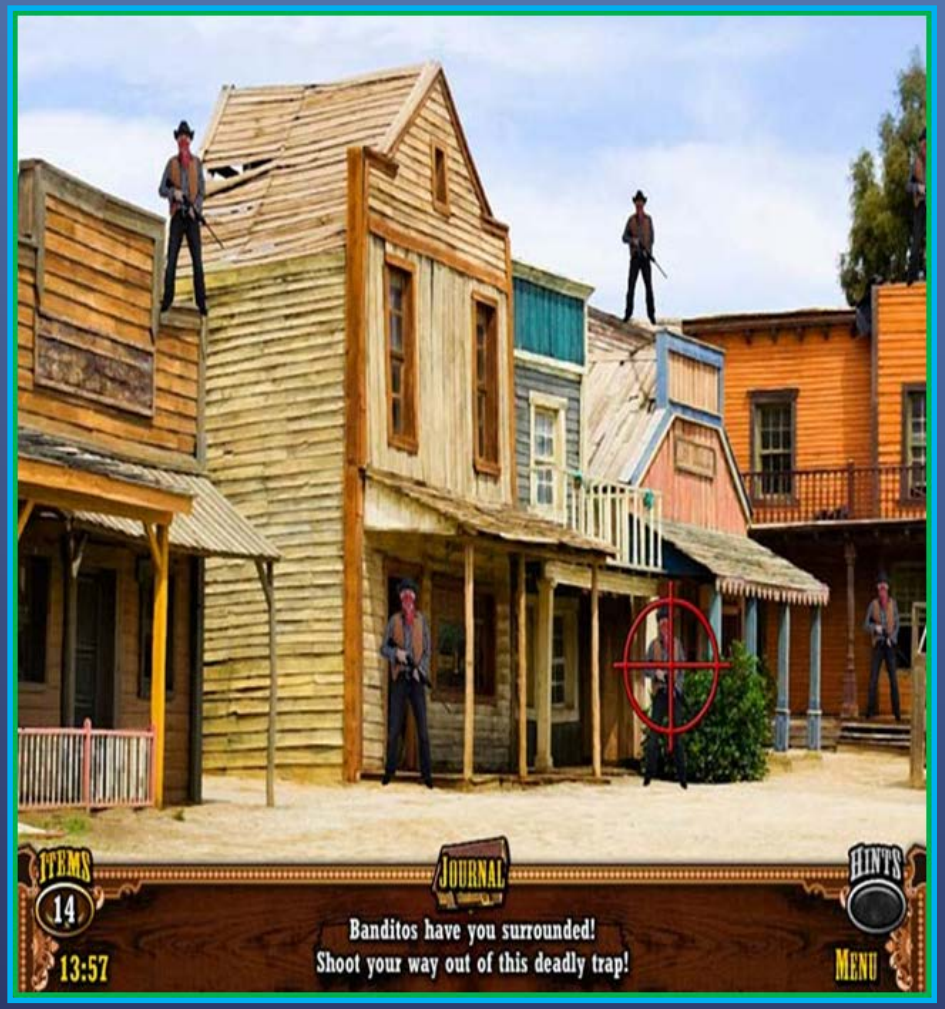
Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"

Відповідно до статті 107 Конституції України, частини другої статті 2 Закону України "Про основи національної безпеки України"
п о с т а н о в л я ю:

UKRANIAN CYBER STRATEGY, MARCH 2016

"APPROVAL OF THE NEW STRATEGY IS INTENDED TO HELP AVOID REPETITION OF HACKER ATTACKS ON THE COUNTRY'S ENERGY FACILITIES, SIMILAR TO THOSE WHICH TOOK PLACE AT THE END OF LAST YEAR ON …ONE OF THE LARGEST ENERGY PROVIDERS IN WESTERN UKRAINE WHICH RESULTED IN AN ENERGY BLOCKADE OF …UKRANIAN ELECTRICITY CONSUMERS."

NATIONAL PERSPECTIVES REFLECT PERCEIVED VULNERABILITIES, SENSITIVITIES AND PRIORITIES.



THE NORM PROBLEM

THE TASK AT HAND:

SETTING CREDIBLE NORMATIVE THRESHOLDS GLOBALLY

THAT INCORPORATE DIVERSE, SOMETIMES OPPOSING, NATIONAL PERSPECTIVES

WHAT INTERNATIONAL LAW DOES FOR A LIVING

1

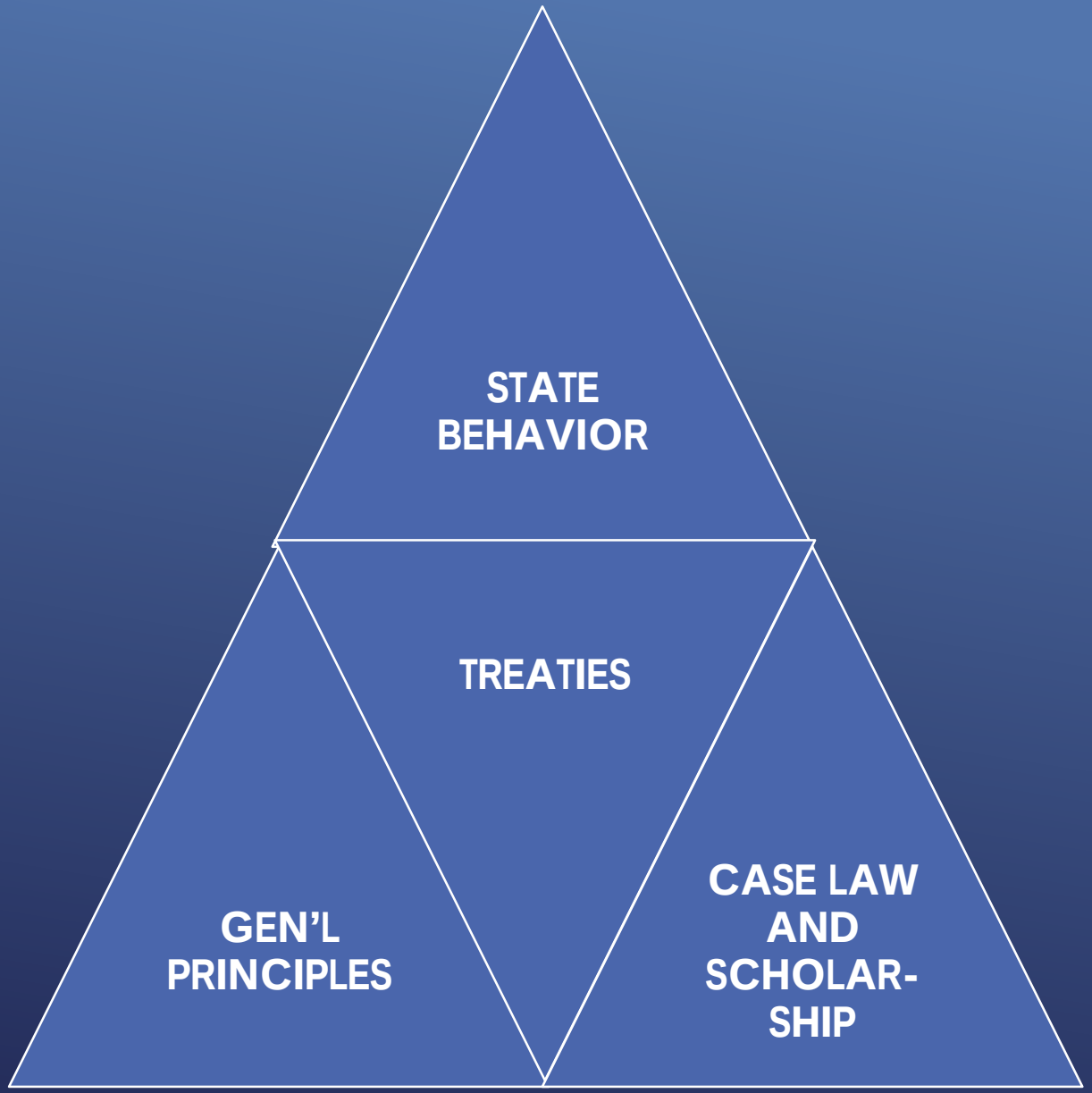
- TAKE INTO ACCOUNT NATIONS' CONCERNS

2

- NEGOTIATE CONCERNS AND INTERESTS and IDENTIFY THE "CUI BONO" ELEMENT

4

- BUILD ENFORCEMENT MECHANISMS



HOW DOES IL WORK?

- NOT PERFECT, BUT…
- IT'S AN IMPORTANT TOOL IN THE TOOLBOX
  - INCENTIVIZES NORMATIVE BEHAVIOR OF STATES
  - WHEN BAD ACTORS PERSIST, THERE ARE MECHANISMS IN PLACE TO SANCTION THEM
- IT'S INTEGRATED INTO AN INTERNATIONAL SYSTEM
- PRECEDENTS: LAW OF THE SEA, NUCLEAR, BIO-CHEM, OUTER SP

AND IN CYBERSPACE FOR THE PAST FEW YEARS

”The most successful tools the federal government has employed so far have been legal ones rather tit-for-tat counterattacks via cyberspace… we should expect to see more of the former.”

--John Carlin, US Ass’t Attorney-Gen’l for National Security, Aug. 1, 2016

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

2016

► G7

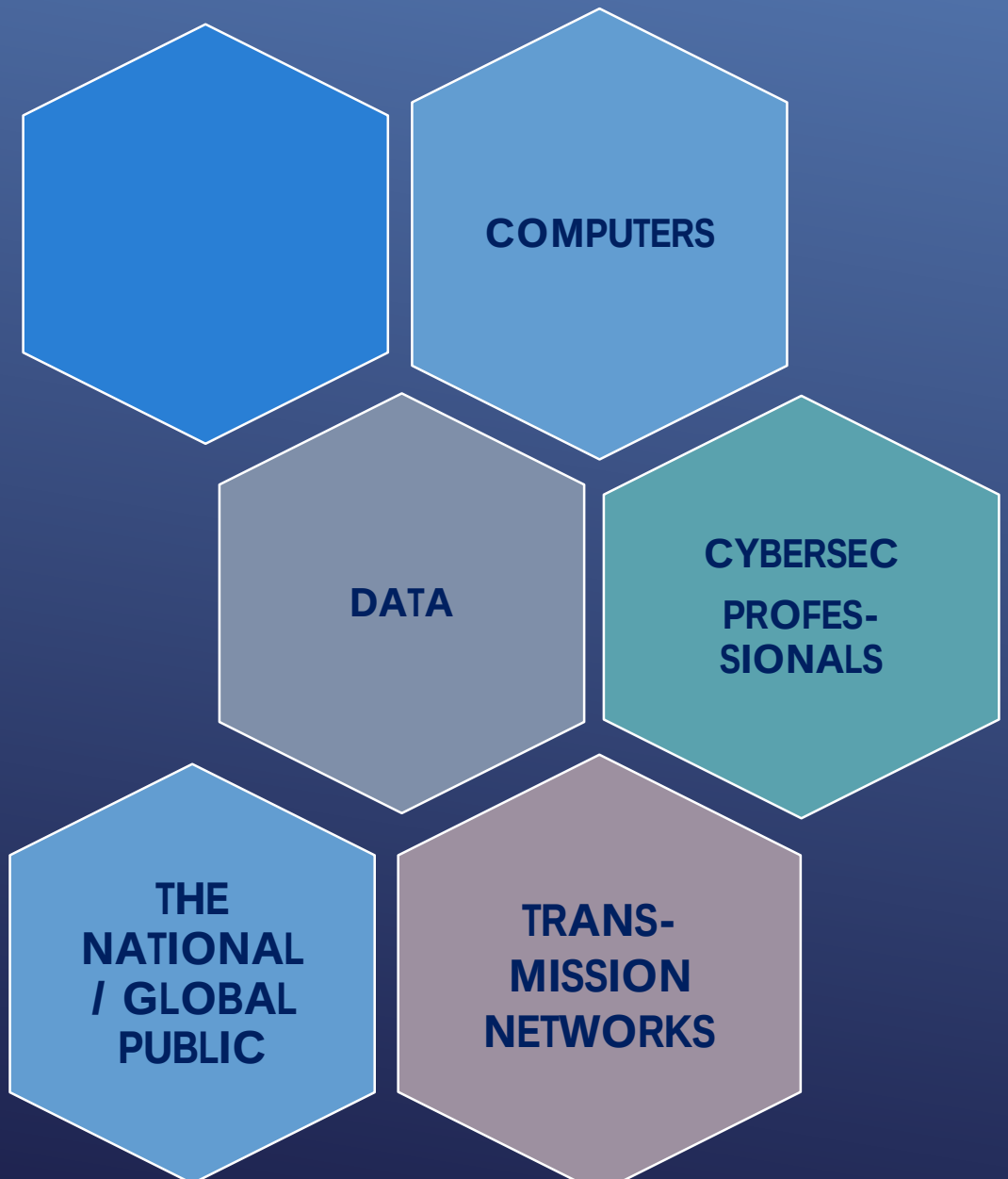
► NATO

► GGE

► TALLINN 2

CONVENTION ON CYBERCRIME, 2001

CYBERSECURITY THREAT VECTORS



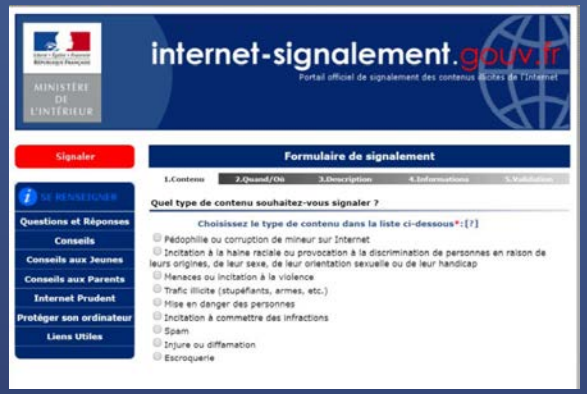
联想
lenovo

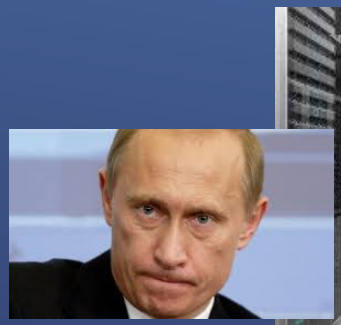
The White House
Office of the Press Secretary

For Immediate Release

Presidential Policy Directive -- United States Cyber Incident Coordination

Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"





"Estonia as a service"

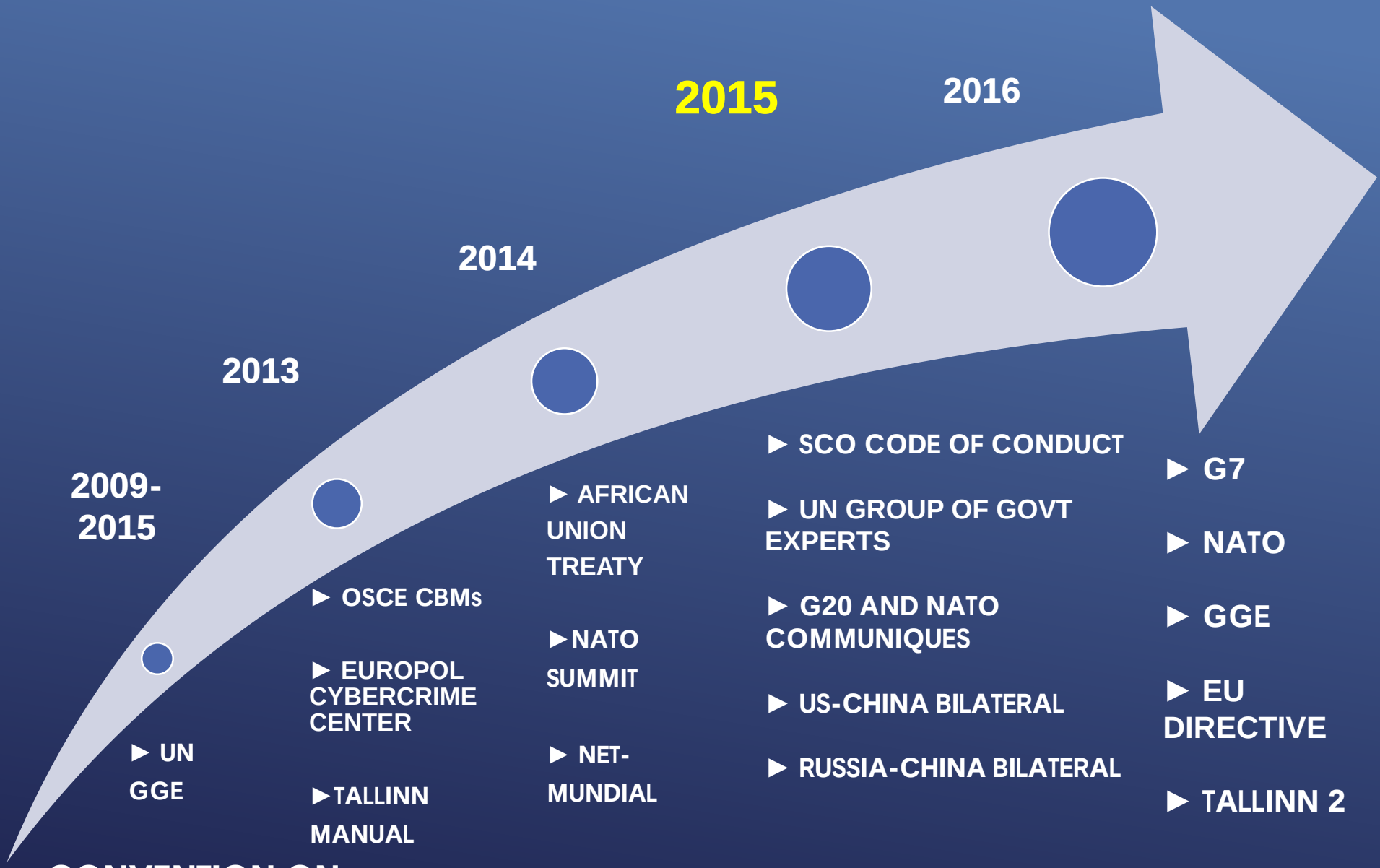
Prime Minister's Office
National Cyber Bureau

משרד ראש הממשלה
מטה הסייבר הלאומי

31 בדצמבר 2015
י"ט בטבת התשע"ו

DIFFERENT VULNERABILITIES >> DIFFERENT FRAMING OF CYBER SECURITY NORMS

“CYBER CANTONIZATION” v. COORDINATED GLOBAL NORMS


2009-2015
► UN GGE
2013
► OSCE CBMs
► EUROPOL CYBERCRIME CENTER
►TALLINN MANUAL
2014
► AFRICAN UNION TREATY
►NATO SUMMIT
► NET-MUNDIAL
2015
► SCO CODE OF CONDUCT
► UN GROUP OF GOVT EXPERTS
► G20 AND NATO COMMUNIQUES
► US-CHINA BILATERAL
► RUSSIA-CHINA BILATERAL
2016
► G7
► NATO
► GGE
► EU DIRECTIVE
► TALLINN 2
CONVENTION ON CYBERCRIME, 2001

United Nations A/70/174

General Assembly

Distr.: General
22 July 2015

Original: English

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

"INFORMATION SECURITY"

- CYBER CODE OF CONDUCT, 2015

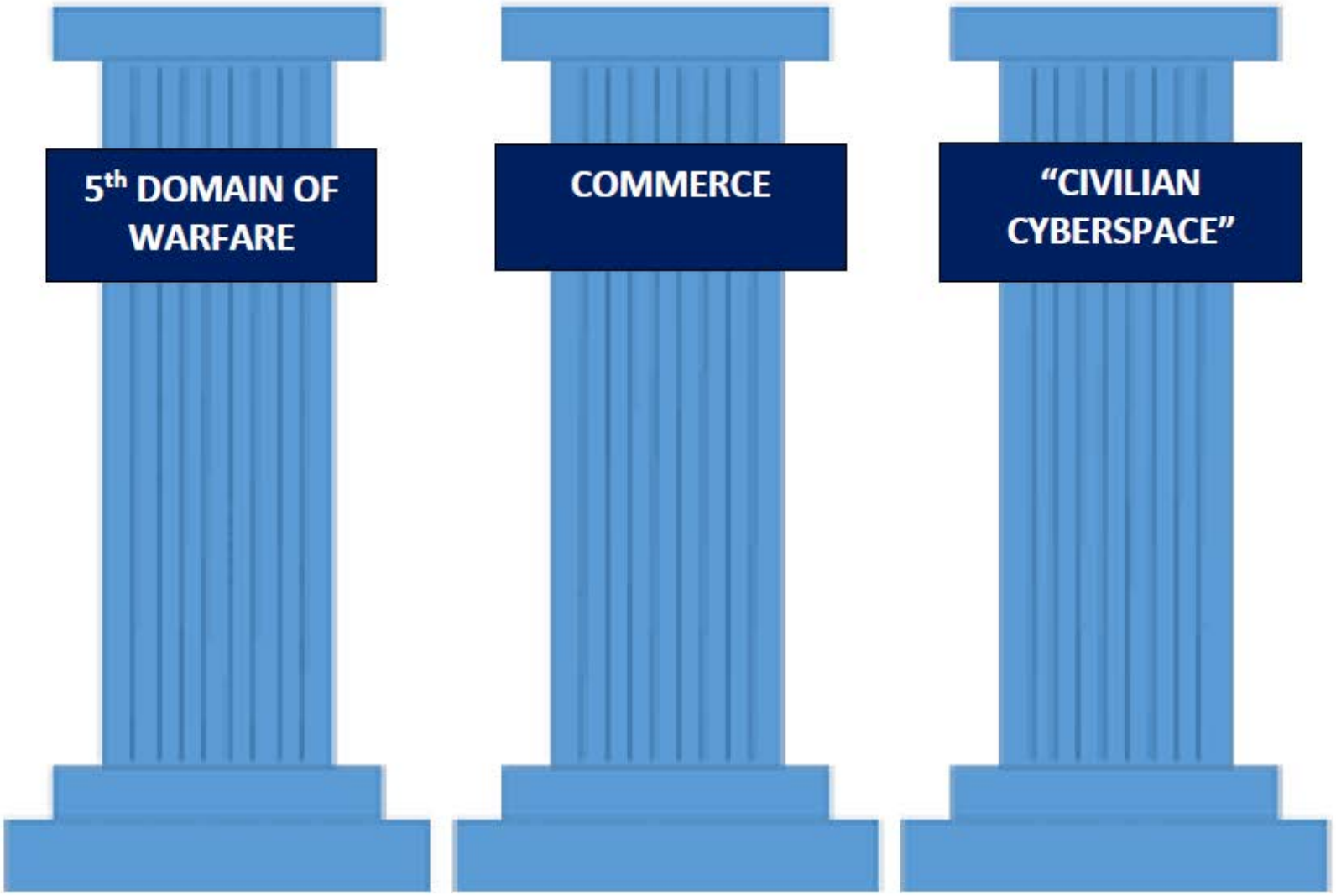
“CREDIBLE DIGITAL SPACE”
“AFRICA’S KNOWLEDGE ECONOMY”

- CONVENTION ON CYBERSECURITY, 2014

- INTERNATIONAL LAW APPLIES TO CYBERSPACE
- INCLUDING COLLECTIVE SECURITY
- STATE RESPONSIBILITY OVER TERRITORIAL INFRASTRUCTURE
- ENFORCEMENT COOPERATION – CERTs, EUROPOL, INTERPOL

TALLIN 2.0

NORMATIVE OUTPUTS


5th DOMAIN OF WARFARE
COMMERCE
"CIVILIAN CYBERSPACE"

PILLAR I : CYBERSPACE AS THE 5TH DOMAIN OF WARFARE

- We affirm that international law, including the United Nations Charter, is applicable in cyberspace.
- We affirm that under some circumstances, cyber activities could amount to the use of force or an armed attack within the meaning of the United Nations Charter and customary international law. We also recognize that states may exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the United Nations Charter and in accordance with international law, including international humanitarian law, in response to an armed attack through cyberspace.

G7 PRINCIPLES AND ACTIONS ON CYBER, 2016

-- CANADA, FRANCE, GERMANY, GB, ITALY, JAPAN, US

-- NATO, ARTICLE 5

ALL MEMBERS SHALL REFRAIN …FROM THE THREAT OR USE OF FORCE AGAINST THE TERRITORIAL INTEGRITY OR POLITICAL INDEPENDENCE OF ANY STATE…

UN 2(4)

NOTHING IN THE PRESENT CHARTER SHALL IMPAIR THE INHERENT RIGHT OF …SELF-DEFENSE IF AN ARMED ATTACK OCCURS AGAINST A MEMBER OF THE UN…

UN 51

"No state can be expected to await an initial attack which…may well destroy the state's capacity for further resistance and so jeopardize its very existence."

Derek Bowett, 1958

"All the News That's Fit to Print"

The New York Times.

LATE CITY EDITION

VOL. CXII...No. 38,258. NEW YORK, TUESDAY, OCTOBER 23, 1962. FIVE CENTS

U.S. IMPOSES ARMS BLOCKADE ON CUBA ON FINDING OFFENSIVE-MISSILE SITES; KENNEDY READY FOR SOVIET SHOWDOWN

U. S. JUDGES GIVEN POWER TO REQUIRE VOTE FOR NEGROES

Chinese Open New Front; Use Tanks Against Indians

Nehru Warns of Peril to Independence —Reds Attack Near Burmese Border and Press Two Other Drives

SHIPS MUST STOP

Other Action Planned If Big Rockets Are Not Dismantled

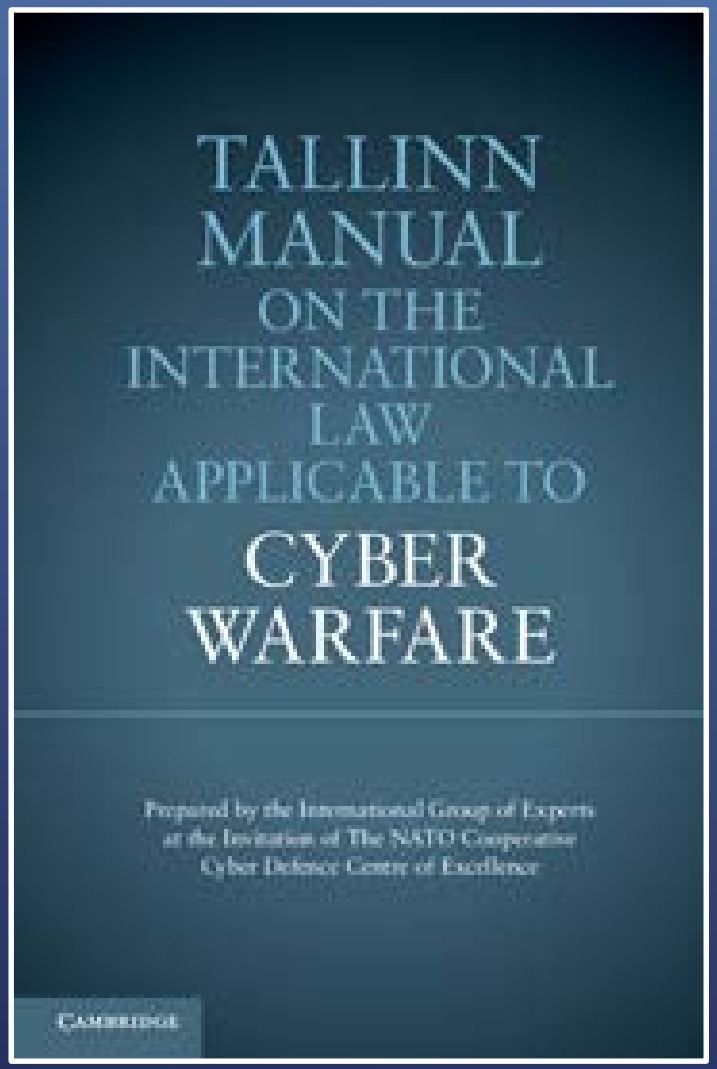
PRESIDENT GRAVE

Asserts Russians Lied and Put Hemisphere in Great Danger

ANTICIPATORY / PRE-EMPTIVE SELF-DEFENCE

- NOT STATES (FOR GOOD REASON)
- LEADING EXPERT AUTHORITIES
- INTERNATIONAL LAW AND COLLECTIVE SECURITY APPLY
- STATES' DE FACTO ACKNOWLEDGEMENT

2013



RULE 11: “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 30: “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.

“THE INTERVIEW” / SONY DATA BREACH, DECEMBER 2013

STATES ARE MORE AND MORE TRANSPARENT ABOUT THEIR OFFICIAL POSITIONS ON THE USE OF FORCE IN CYBERSPACE

"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

"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

(1) INTERNATIONAL LAW APPLIES

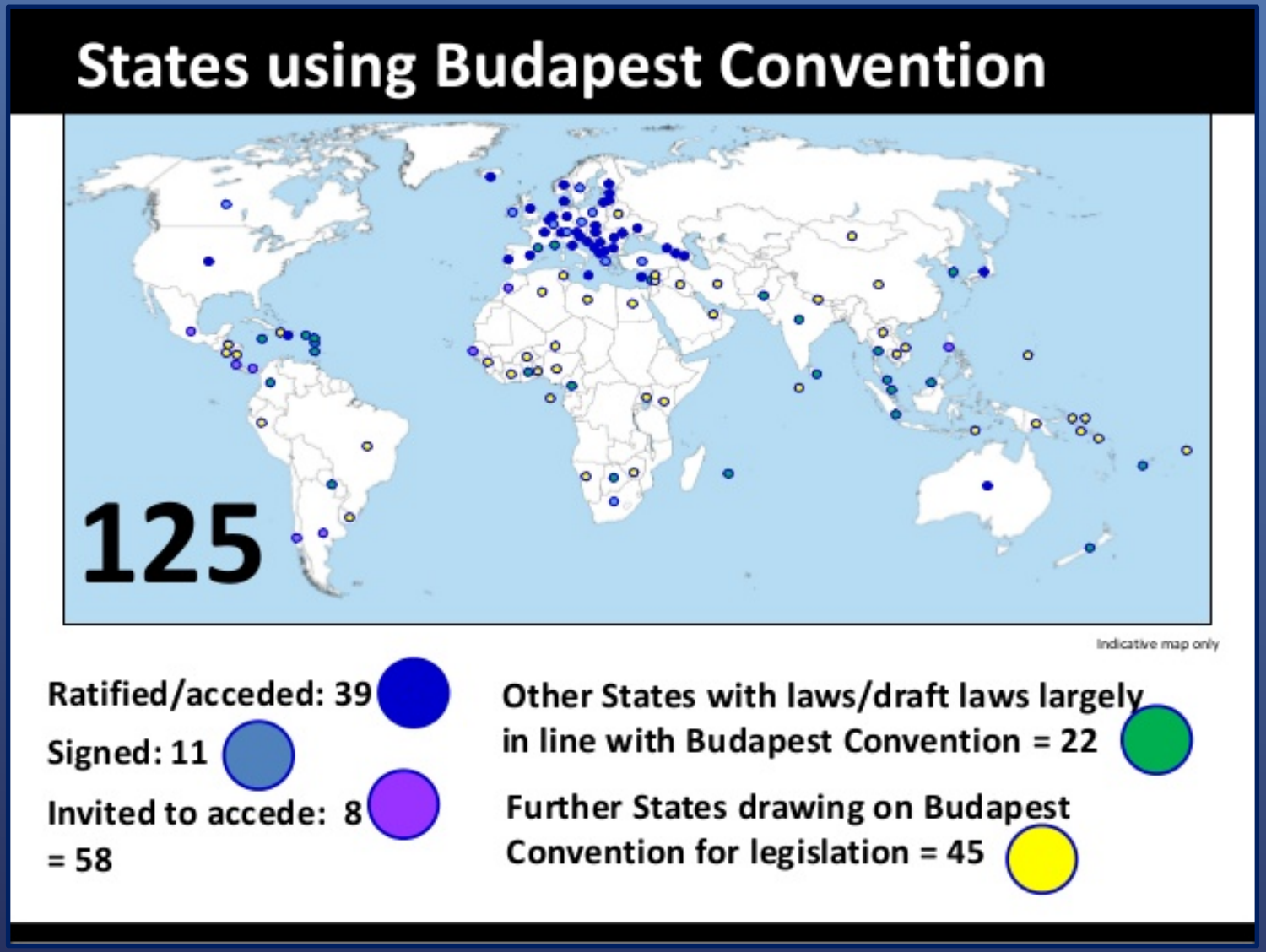
(2) "SCALE AND EFFECTS TEST" FOR SELF-DEFENSE TO BE JUSTIFIED

(3) SOME DECLARATIONS-

TRANSPARENT STATE PRACTICE LACKING

SUMMARY OF PILLAR I : THE 5TH DOMAIN OF WARFARE

PILLAR II : “CIVILIAN CYBERSPACE” SECURITY



2001 BUDAPEST CONVENTION ON CYBERCRIME

THE PARTIES SHALL AFFORD ONE ANOTHER MUTUAL ASSISTANCE TO THE WIDEST EXTENT POSSIBLE FOR THE PURPOSE OF INVESTIGATIONS OR PROCEEDINGS CONCERNING CRIMINAL OFFENCES RELATED TO COMPUTER SYSTEMS AND DATA, OR FOR THE COLLECTION OF EVIDENCE IN ELECTRONIC FORM OF A CRIMINAL OFFENCE.

ART. 25

- INTERPOL
- EUROPOL
- FBI
- SECTORAL (BANKS, FINANCE)

24/7 PoC
NETWORK MANDATED

CYBER POLICING HAS GONE GLOBAL

(1) CYBERCRIME CONVENTION MANDATES MUTUAL ASSUSTANCE

(2) CYBERCRIME DEFINITIONS

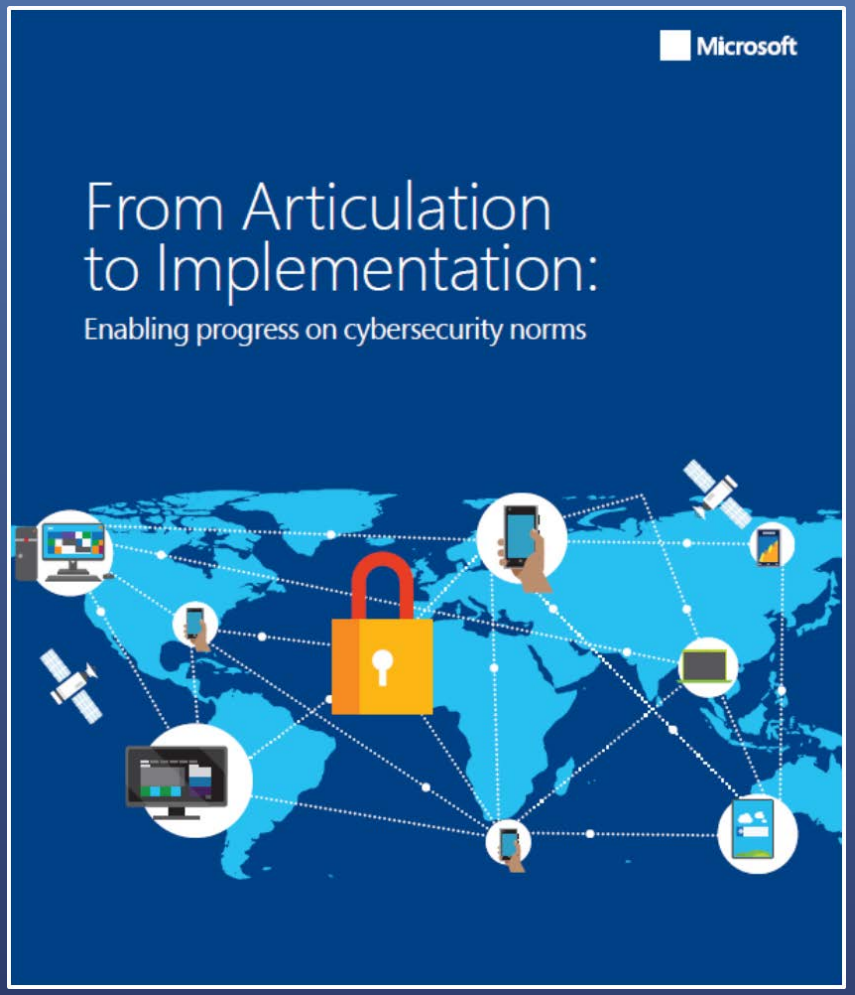
(3) REQUIRED PoC ALERTS

+ POLICING

SUMMARY OF PILLAR II : “CIVILIAN CYBERSPACE” SECURITY

PILLAR III : CHANGING ROLE OF COMMERCIAL STAKEHOLDERS IN DETERMINING INTERNATIONAL NORMS

STAKEHOLDERS HAVE CHANGED AT THE GLOBAL LEVEL



CHANGING AND UNPRECEDENTED ROLES FOR TRANSNATIONAL COMMERCIAL ENTITIES

INDUSTRY MUST ALSO HAVE AN AVENUE TO CONTRIBUTE TO NORMS IMPLEMENTATION…INDUSTRY OFTEN HAS TECHNICAL INFORMATION THAT CAN IMPROVE THE THRESHOLD DETERMINATION OF WHETHER AN ATTACK WAS LAUNCHED BY A NATION-STATE.

…INDUSTRY IS OFTEN BEST POSITIONED TO IDENTIFY THE KEY LESSONS FROM NATION-STATE ATTACKS…

(1) GLOBAL STAKEHOLDERS ARE CHANGING

(2) TRANSNATIONAL INFLUENCE OF COMMERCE IS UNPRECEDENTED

(3) ROLE IN POLICY AND LAWMAKING - TBD

SUMMARY OF PILLAR III : CHANGING ROLE FOR COMMERCIAL STAKEHOLDERS

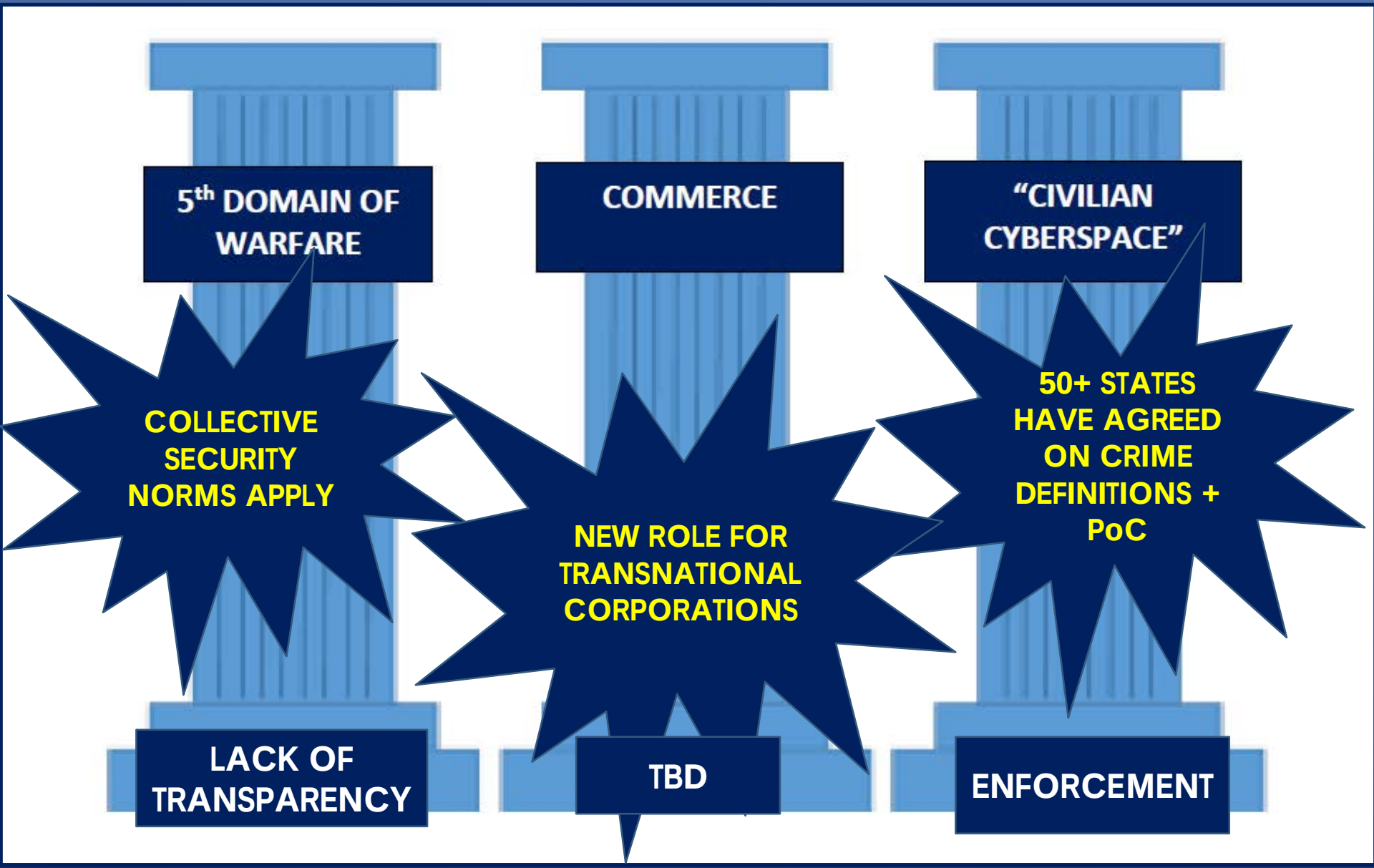
SUMMING UP: TRENDS AND OUTCOMES

THE TASK AT HAND

TO SET

CREDIBLE NORMATIVE THRESHOLDS GLOBALLY

THAT INCORPORATE DIVERSE, SOMETIMES OPPOSING, NATIONAL PERSPECTIVES


5th DOMAIN OF WARFARE
COMMERCE
"CIVILIAN CYBERSPACE"
COLLECTIVE SECURITY NORMS APPLY
NEW ROLE FOR TRANSNATIONAL CORPORATIONS
50+ STATES HAVE AGREED ON CRIME DEFINITIONS + PoC
LACK OF TRANSPARENCY
TBD
ENFORCEMENT

DE-SILO

INTEGRATE INTO OTHER AREAS OF INT'L LAW

3 CRITICAL CHALLENGES

- CYBERTERRORISM
- INFRASTRUCTURE PROTECTION
- WHAT IS DATA?

COORDINATED GLOBAL NORMS – THE WAYS AHEAD

THANK YOU.

deborah@cyberregstrategies.com

01100100 01100101 01100010 01101111 01110010 01100001 01101000 01000000 01100011 01111001 01100010 01100101 01110010 01110010 01100101
01100111 01110011 01110100 01110010 01100001 01110100 01100101 01100111 01101001 01100101 01110011 00101110 01100011 01101111 01101101

DE-SILO

INTEGRATE INTO OTHER AREAS OF INT'L LAW

3 CRITICAL CHALLENGES

- CYBERTERRORISM
- INFRASTRUCTURE PROTECTION
- DATA

COORDINATED GLOBAL NORMS – THE WAYS AHEAD