

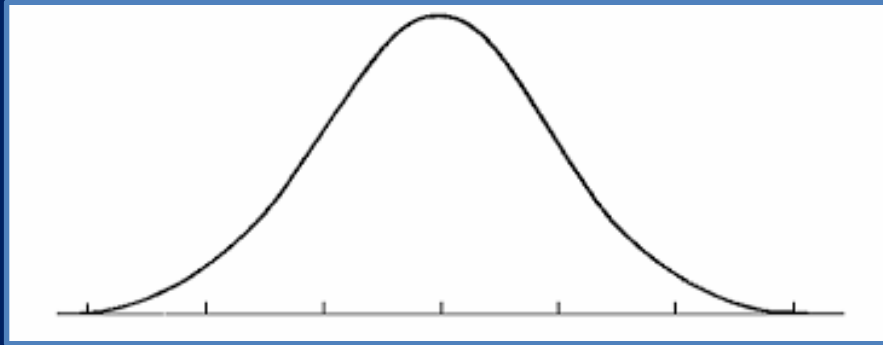
ICT WORLD SUMMIT ON COUNTER-TERRORISM: THE TERRORISM MAZE

COUNTER-TERRORISM BY REGULATION:

CYBERIZING NATIONAL LAWS AND THE TREND TOWARDS PUBLIC- PRIVATE INFORMATION SHARING

Deborah Housen-Couriel, Adv.
ICT Fellow
September 5, 2018

HOSTILE USES / ABUSES OF THE INTERNET

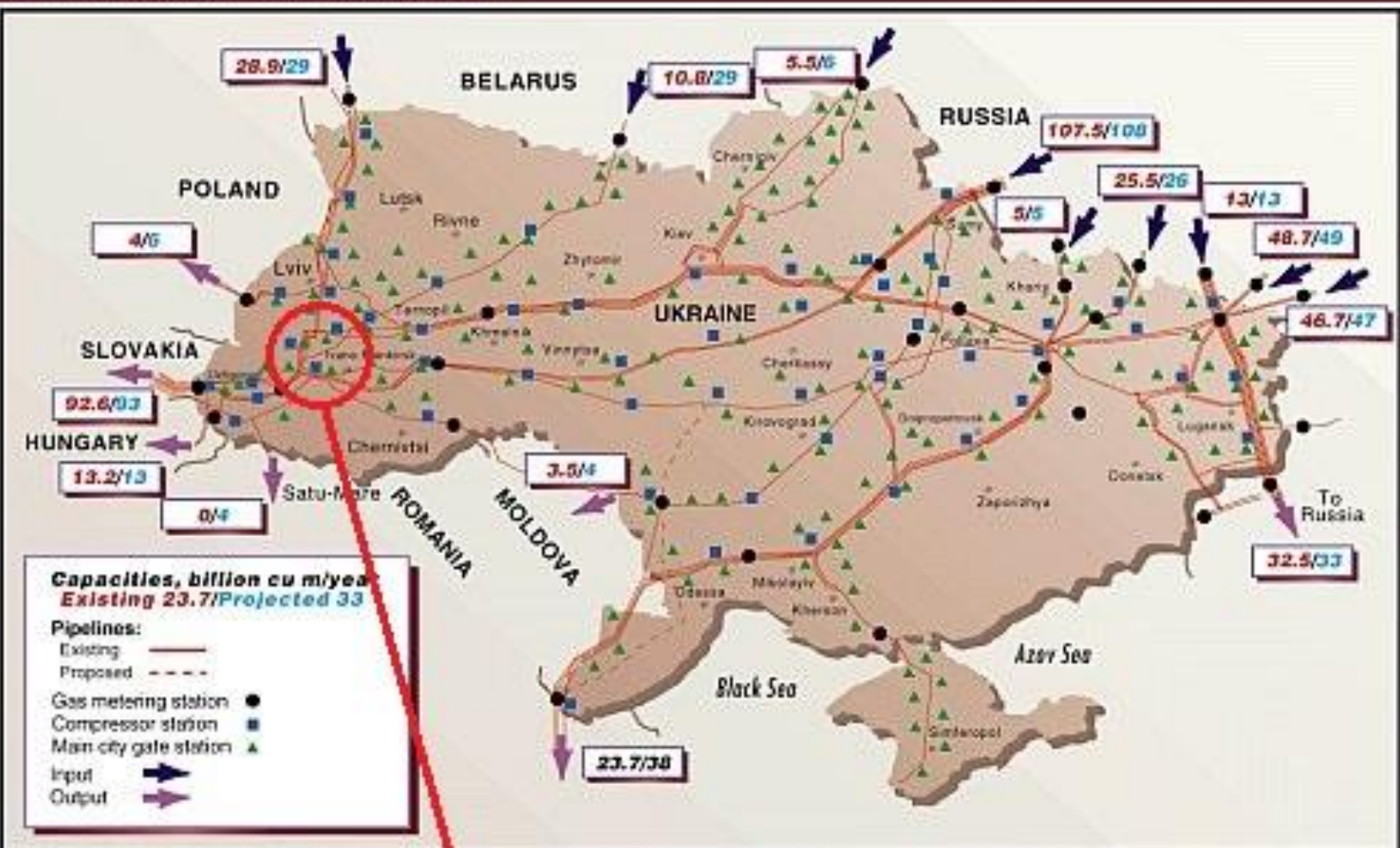


- CYBER TERRORISM
 - CYBER ESPIONAGE
 - CYBER CRIME
 - CYBER ATTACKS
 - CYBER WARFARE
-
- **UNTIL RECENTLY -
NORMATIVE
AMBIGUITY**

December 2015 – 1st CYBER-ENABLED CIVILIAN INFRASTRUCTURE HACK



UKRAINE'S GASTRANSMISSION SYSTEM *



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

doi:10.1017/S002229240000191

Location of power system outage



**AN ACT OF
WAR B/W
STATES**

**ISSUE FOR
THE UN
SECURITY
COUNCIL**

**CYBER
TERRORISM**

**CYBER
CRIME
WITHOUT A
TERRORIST
ELEMENT**

ESPIONAGE

**BUSINESS
CONTINUITY
ISSUE**

EVEN WHEN WE HAVE NORMATIVE CLARITY: ENFORCEMENT CHALLENGES

Home > Israel News

Egypt's Cyber-ops Against ISIS Jams Israeli Cellular Networks

In recent weeks the Egyptian military has been waging a major campaign against the Islamic State fighters in Egypt's Sinai Peninsula

Yaniv Kubovich and The Associated Press | Mar 07, 2018 2:38 PM

ENFORCEMENT CHALLENGES (2)

NEW
PERSONAL
DATA
PROTECTION
LAWS

GDPR



Data Protection
Officer (DPO)



Compliance



25 May 2018



Data Breaches



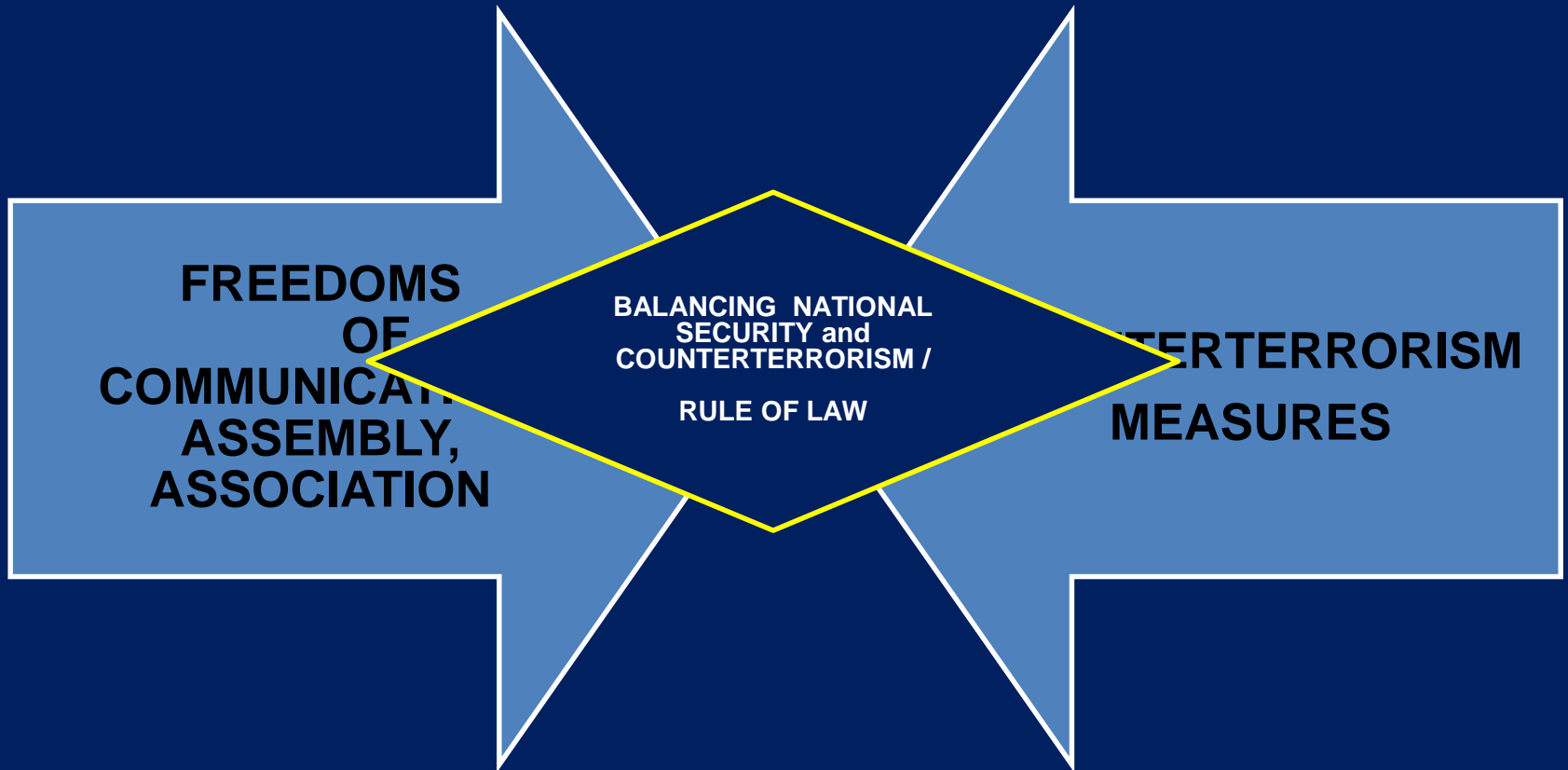
Personal Data

CHINA

INDIA

RUSSIA

ENFORCEMENT CHALLENGES (3)



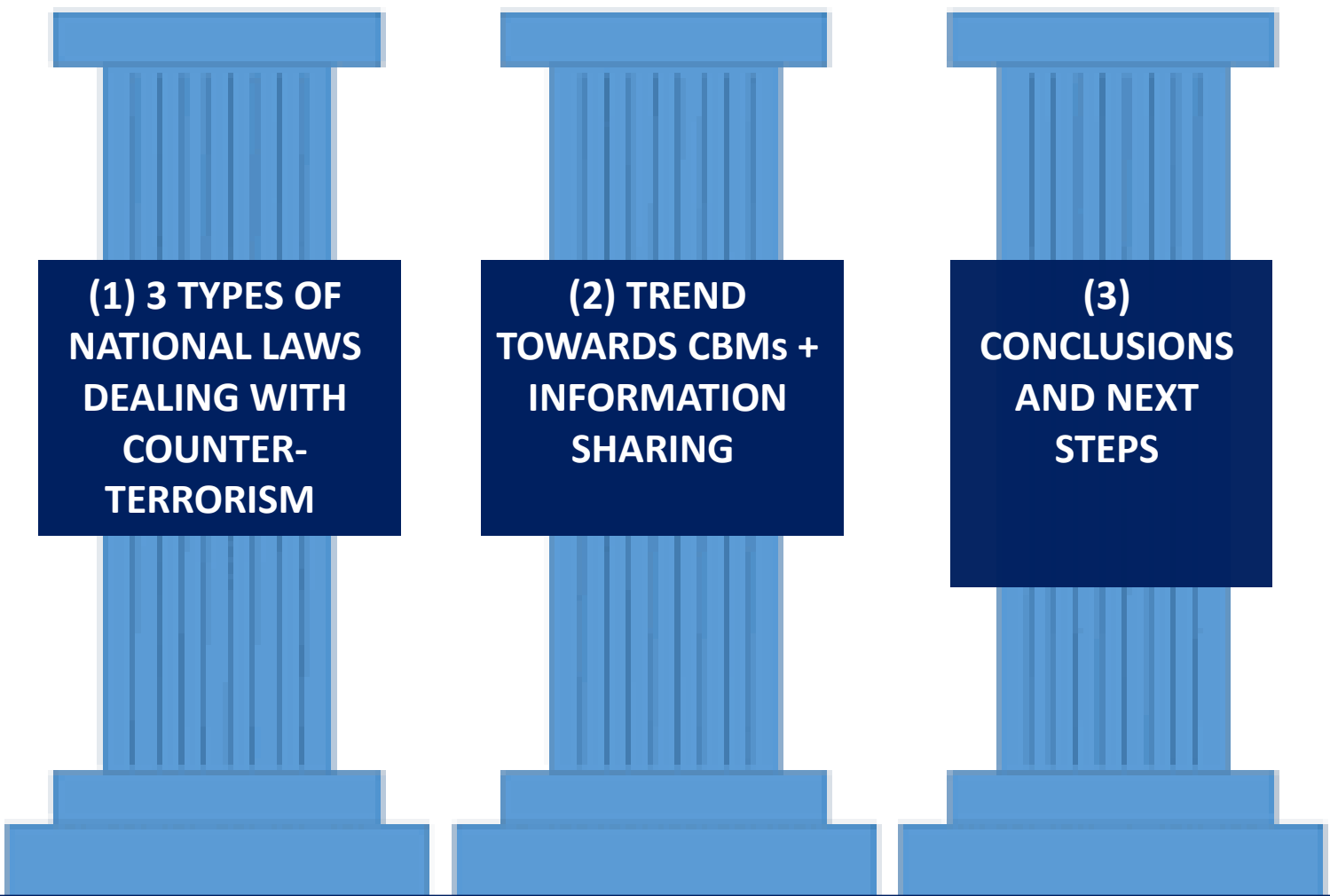
HOW DO NATIONAL LAWS CURRENTLY **ADDRESS THIS NORMATIVE CONFUSION AND CONTRIBUTE TO COUNTER-TERRORISM EFFORTS?**



INCLUDING
ENFORCEMENT

SPOILER ALERT

- THROUGH **3 TYPES OF COUNTER-TERRORISM LAWS**
- AND THROUGH CONFIDENCE-BUILDING MEASURES (**CBM'S**) SUPPORTING THESE LAWS
 - ESPECIALLY **INFORMATION SHARING** FOR EXCHANGE OF STRATEGIC AND ACTIONABLE COUNTER-TERRORIST INTELLIGENCE
 - **WHAT'S NEW:** THE **PRIVATE SECTOR** PLAYS AN ACTIVE PART IN THIS INFORMATION SHARING



**(1) 3 TYPES OF
NATIONAL LAWS
DEALING WITH
COUNTER-
TERRORISM**

**(2) TREND
TOWARDS CBMs +
INFORMATION
SHARING**

**(3)
CONCLUSIONS
AND NEXT
STEPS**

**TERRORIST
LEVERAGE
and USE OF
THE
INTERNET**

A Venn diagram with two overlapping circles. The left circle is labeled 'TERRORIST LEVERAGE and USE OF THE INTERNET'. The right circle is labeled 'CYBER – ENABLED TERRORISM'. Below the left circle is a blue diamond containing the text 'Financing, propaganda, recruitment, INCITEMENT'. Below the right circle is a blue diamond containing the text 'Physical damage or attempt to damage'. The intersection of the two circles is empty.

**Financing,
propaganda,
recruitment,
INCITEMENT**

**CYBER –
ENABLED
TERRORISM**

**Physical
damage or
attempt to
damage**

KEY DISTINCTION IN THE LAW

“Cyber-enabled terrorism” involves acts intentionally committed by any person who

- **uses information and communication technologies** unlawfully in ways that cause, or are intended to cause, death or serious bodily injury to persons,
- **substantial damage to public or private property, the economy, or the environment, or serious disruption of public services and**
- **that are undertaken with the intent to spread fear in civilian populations or to compel a government, a civilian population, or an international organization to take or abstain from specific acts...**

STARTING POINT:

ILA WORKING DEFINITION, 2016

(1) NATIONAL LAWS DEALING WITH CYBER-ENABLED TERRORISM

THE ISRAELI EXAMPLE

HOSTILE CYBER ATTACKS ON ISRAEL ARE ONGOING

- Wars with in the Gaza Strip with Hamas
 - Summer 2018: World Cup honeypot
 - Protective Edge, 2014
 - Pillar of Fire, end of 2012
 - Cast Lead, 2009
- Iran hostile activity
- “Anonymous” threats and hostile activity- Passover 2015
- Delegitimization of Israel, BDS, student movements

2012 WAKEUP CALL: OXOMAR, THE SAUDI HACKER



- 15,000 Israelis – credit card data, 3 co's
- to "...hurt Israel -- politically, economically and culturally"
- "I will finish Israel electronically"
- Stormy public debate
- Beginning of awareness of cyber vulnerability

- **Motivation** is political, religious, nationalistic, or ideological
- Carried out **with the goal of causing public fear** or alarm, or to cause the government or another public body (in Israel or abroad, including IOs) to either act or refrain from acting
- **One of the following** was either threatened or had a real danger of occurring:

COMBATTING TERRORISM LAW, 2016
DEFINING “ACT OF TERRORISM”



- 1) Severe injury to **a person's body or freedom**;
- 2) Severe injury to **public safety or health**
- 3) Severe damage to **property**
- 4) Severe damage to **religious objects, places of worship** or other sites
- 5) Severe damage to **infrastructure, systems or basic services, or severe interference with them, or severe damage to the national economy or ecosystem.**

TOWARDS A **BROADER DEFINITION** ON THE PART OF ISRAEL'S LEGAL SYSTEM AND LAW ENFORCEMENT AS TO WHAT CONSTITUTES A “TERRORIST ACT”



AND ITS
ENCOMPASSING OF
CYBER-ENABLED
TERRORISM

3 NATIONAL REGULATORY STRATEGIES FOR CYBERIZATION OF COUNTER-TERRORISM LAWS

(1) RESULTS-ORIENTED APPROACH

- Countries which have set counter-terrorism laws and have defined acts of terrorism therein, yet have **refrained from specifying a typology of such cyber-enabled terrorist acts** and have adopted a results-oriented approach.
- Any criminal act that culminates in a specified result as defined by the law's criteria will constitute an act of terrorism – whether cyber-enabled or not. Laws in this category of legislation **refrain from stipulating terrorist acts that leverage cyber tools in particular**, but neither do they exclude them.

- 1) Severe injury to **a person's body or freedom;**
- 2) Severe injury to **public safety or health**
- 3) Severe damage to **property**
- 4) Severe damage to **religious objects, places of worship** or other sites
- 5) Severe damage to **infrastructure, systems or basic services, or severe interference with them, or severe damage to the national economy or ecosystem.**



CANADA

INDIA



SIMILAR “RESULTS-ORIENTED” COUNTER-TERRORISM LAWS (NOT “CYBERIZED”)

(2) INDIRECT APPROACH

The second group of countries have adopted an approach of **indirect categorization of already-criminalized acts as “terrorism”**.

- In these cases, exemplified by the German and US criminal codes, **existing criminal acts are additionally categorized as acts of terror under a specific counter-terrorism provision**
- Increasing the severity of punishment when the act is committed in conformity with additional criteria, such as the intent to terrorize the public or to coerce a public authority.
- Both the German and the US codes classify **unauthorized access** to computers and computer systems as such acts.



POLITICS

White House won't defend
GOP leaders...



POLITICS

Lawmakers request full
report on Trump sec...



POLITICS

GOP shifts from tax overhaul
to cuts befor...



INSIDE THE BELTWAY

Nostalgia: national
\$9 trillion i...

HOME \ NEWS \ SECURITY


Islamic State hacker sentenced for assisting terrorist group with 'kill list'



THE ARDIT FERIZI CASE, 2016



Ardit Ferizi leaked data included names, e-mail addresses, passwords, locations and phone numbers of **1,351 U.S. military and other government personnel.**



“We are in your emails and computer systems, watching and recording your every move, we have your names and addresses, we are in your emails and social media accounts, **we are extracting confidential data and passing on your personal information to the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands!”**

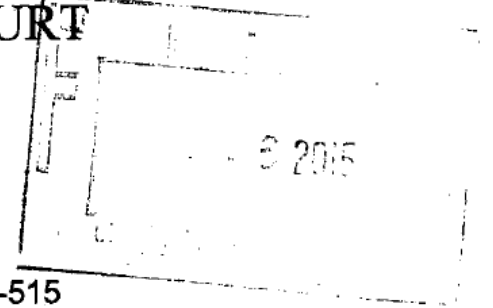
**Islamic State
Hacking Division
tweet**

This case represents the first time we have seen the very real and dangerous national security cyber threat that results from **the combination of terrorism and hacking..**

**US DEPARTMENT OF JUSTICE-
“GROUNDBREAKING”**

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



United States of America

v.

ARDIT FERIZI
a/k/a Th3Dir3ctorY,

Case No. 1:15-MJ-515

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

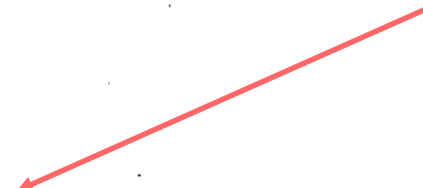
On or about the date(s) 4/01/15 to or on about 8/11/15 in the extraterritorial jurisdiction of U.S. and in the
Eastern District of Virginia, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. § 1030
18 U.S.C. § 1028A
18 U.S.C. § 2339B

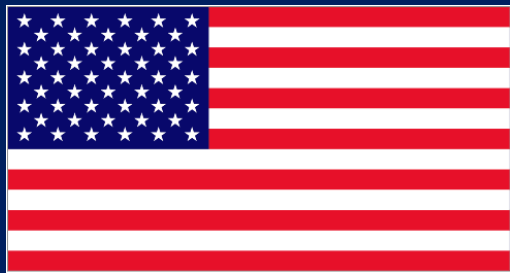
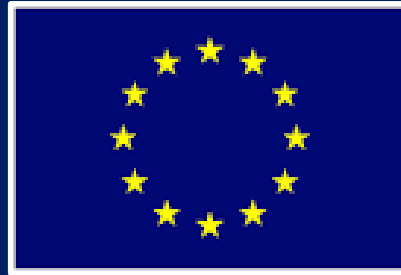
Unauthorized access to a computer;
Aggravated identity theft; and
Providing material support to a designated foreign terrorist group



(3) CYBERIZED LAWS

Thirdly, several countries have opted for legislative provisions that specifically address cyber-enabled terrorism – these are the “cyberized” definitions of terrorist acts.

- Certain types of interference with computer systems and electronic communications are explicitly defined as acts of terrorism.
- Recognition of these vulnerabilities.



WHO'S CYBERIZED?

(f) [An act which] seriously interferes with, **seriously disrupts, or destroys, an electronic system** including, but not limited to:

- an **information system**; or a
- **telecommunications system**; or a
- **financial system**; or a
- system used for the **delivery of essential government services**; or a
- system used for, or by, **an essential public utility**; or a
- system used for, or by, **a transport system**.

AUSTRALIA CRIMINAL CODE "TERRORIST ACT "



2) Action falls within this subsection if it—

(a) involves serious violence against a person,

(b) involves serious damage to property,

(c) endangers a person's life, other than that of the person committing the action,

(d) creates a serious risk to the health or safety of the public or a section of the public, or

(e) is designed seriously to interfere with or seriously to disrupt an electronic system.

UK TERRORISM ACT



- ▶ A terrorist act shall likewise refer to any conduct committed with the intent to achieve, prepare, or instigate one of the purposes set out in the first paragraph of this article, if it is as such **to harm communications, information, financial or banking systems**, national economy, energy reserves, security stock of goods, food and water, or their integrity, or medical services in disasters and crises.

EGYPT'S LAW ON COMBATTING TERRORISM, 2015



DIRECTIVE (EU) 2017/541 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 15 March 2017
on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending
Council Decision 2005/671/JHA



TERRORIST OFFENCES AND OFFENCES RELATED TO A TERRORIST GROUP

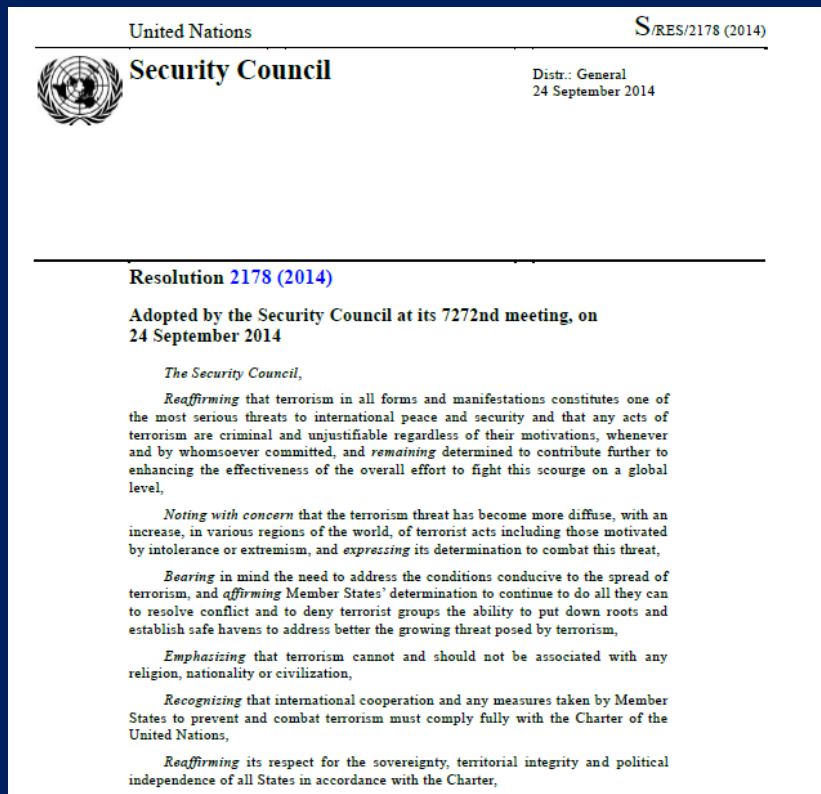
Article 3

Terrorist offences

1. Member States shall take the necessary measures to ensure that the following intentional acts, as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, are defined as terrorist offences where committed with one of the aims listed in paragraph 2:

- (a) attacks upon a person's life which may cause death;
- (b) attacks upon the physical integrity of a person;
- (c) kidnapping or hostage-taking;
- (d) causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;

AT THE GLOBAL LEVEL: UNSC 2178 (2014)



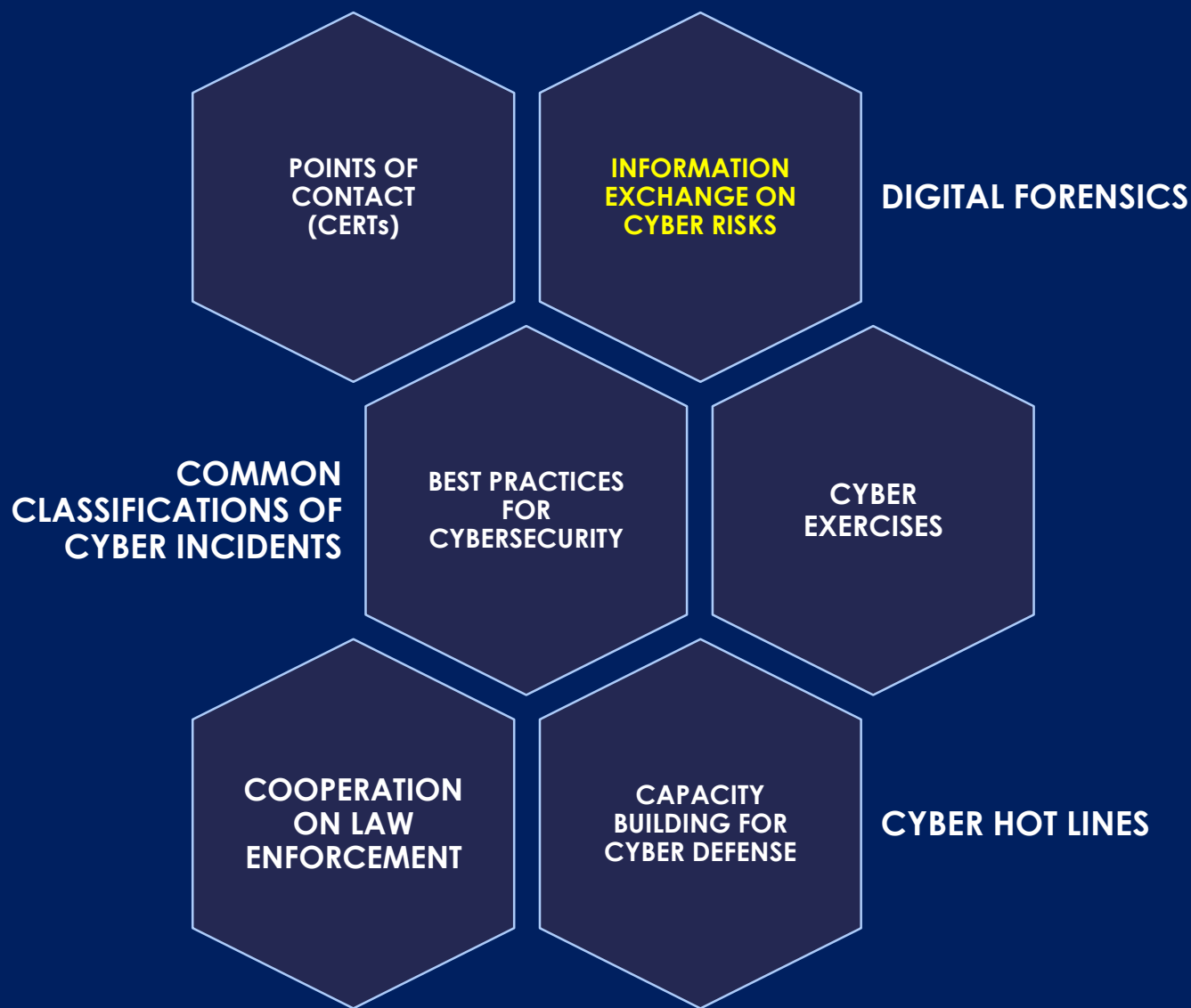
Expressing concern over the increased use by terrorists and their supporters of communications technology for the purpose of radicalizing to terrorism, recruiting and inciting others to commit terrorist acts, including through the internet, and financing and facilitating the travel and subsequent activities 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,

**(2) TREND TOWARDS CBMs + INFORMATION
SHARING**

▶ INTERNATIONAL **COOPERATION**
NECESSARY IN CYBERSPACE FOR
ENFORCEMENT OF THESE LAWS

▶ CBM's ARE HELPING TO BUILD **A**
BASIS FOR GLOBAL
IMPLEMENTATION

**ENFORCING NATIONAL
COUNTER-TERRORISM LAWS**



CONFIDENCE BUILDING MEASURES (CBM'S)



ASEAN REGIONAL FORUM



Group of Governmental Experts



► 24/7 PoCs FOR INFORMATION EXCHANGE ON ALERTS

► INTER

► EURO

► SECT
LAUN



CYBER POLICING HAS GONE GLOBAL

- ▶ IN THE **NATIONAL LICENSES** OF CRITICAL INFRASTRUCTURES
- ▶ MANDATED USE OF **ISACs** (Information Sharing and Analysis Centers)
- ▶ **SECTORAL PLATFORMS**: FINANCIAL AND HEALTH

IS REGARDING CYBER THREATS OF ALL TYPES – INCLUDING TERRORIST ACTS – IS **INCREASINGLY MANDATED BY NATIONAL REGULATORS**

[HOME](#)[ABOUT](#)[COUNTRIES](#)[PUBLICATIONS](#)[Calendars](#)[EN](#)[FR](#)[Home](#) / [Publications](#) / [FATF Recommendations](#)/ [International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations](#)

International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations

[Send](#)[Print](#)[Tweet](#)[FATF Recommendations 2012](#)[Download pdf \(990kb\)](#)

SECTORAL INFORMATION SHARING: FINANCIAL ACTION TASK FORCE

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



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

WHAT'S NEW: CHANGING AND UNPRECEDENTED ROLES FOR NON-STATE ACTORS

Facebook, Microsoft, YouTube and Twitter form Global Internet Forum to Counter Terrorism

John Mannes @johnmannes / Jun 26, 2017

 Comment



Global Internet Forum to Counter Terrorism

VISION

ABOUT

LEADERSHIP

PARTNERS

PRESS

The vision of the GIFCT is to prevent terrorists from exploiting our platforms.

Terrorism is an attack on open societies and addressing the threat posed by violence is a critical challenge for all of us. Our companies have amassed considerable experience in tackling extremist and violent content on our platforms, and we are committed to playing our part in addressing this global challenge — together with governments and civil society groups, which address the problem on the ground every day.

- ▶ **Joint database for unique digital "fingerprints" for violent terrorist imagery or terrorist recruitment videos** that we have removed from our services. By sharing these 50,000 hashes with one another, we can identify potential terrorist images and videos on our respective hosted consumer platforms. This collaboration is resulting in increased efficiency as we continue to enforce our policies to help curb the pressing global issue of terrorist content online.

A SHARED INDUSTRY DATABASE OF "HASHES"

- ▶ **Knowledge sharing** is one of the key areas of focus for the GIFCT. One of the GIFCT's key partners in enhancing our work in this area is Tech Against Terrorism.
- ▶ Tech Against Terrorism is a **public-private partnership** which was originally launched by the United Nations Counter-Terrorism Executive Directorate (UN CTED) in 2016.

PARTNERSHIP WITH “TECH AGAINST TERRORISM”



Welcome to the Knowledge Sharing Platform

The Knowledge Sharing Platform (KSP) is a resource available to members of the Tech Against Terrorism initiative





Royal United Services Institute



International Institute for Counter-Terrorism (ICT)

**NEW RESEARCH INTO THESE PLATFORMS AND
HOW THEY SUPPORT REGULATORY EFFORTS
AGAINST CYBERTERRORISM**

- ▶ **SUPPORT FOR ENFORCEMENT** OF ALL 3 TYPES OF LAWS TO COMBAT CYBER TERRORISM
- ▶ INCREASINGLY **REQUIRED** OF PRIVATE SECTOR COMPANIES
- ▶ **RULE OF LAW CRITIQUE:** NOT TRANSPARENT

NEW PUBLIC-PRIVATE PARTNERSHIPS TO SHARE ACTIONABLE INTELLIGENCE FOR COUNTER-TERRORISM

(3) CONCLUSIONS AND NEXT STEPS

National
legislation is
evolving in **3**
ways:

results-
oriented,
indirect
approach,
cyberized



**Information-
sharing** is
supporting
international
cooperation
to implement
these laws



More
engagement
and leverage
of **private-
sector actors**
through
partnerships
with
governments

IN SUMMARY

LEGAL NORMS NEED TO BE GLOBALIZED



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,

Emphasising 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,

“...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”

- ▶ The **next substantive challenge** and a question for discussion:
- ▶ Cyber-enabled **influence campaigns** and manipulation including elections
- ▶ **Should we include in definitions of terrorism?**



ANY QUESTIONS?

THANK YOU.