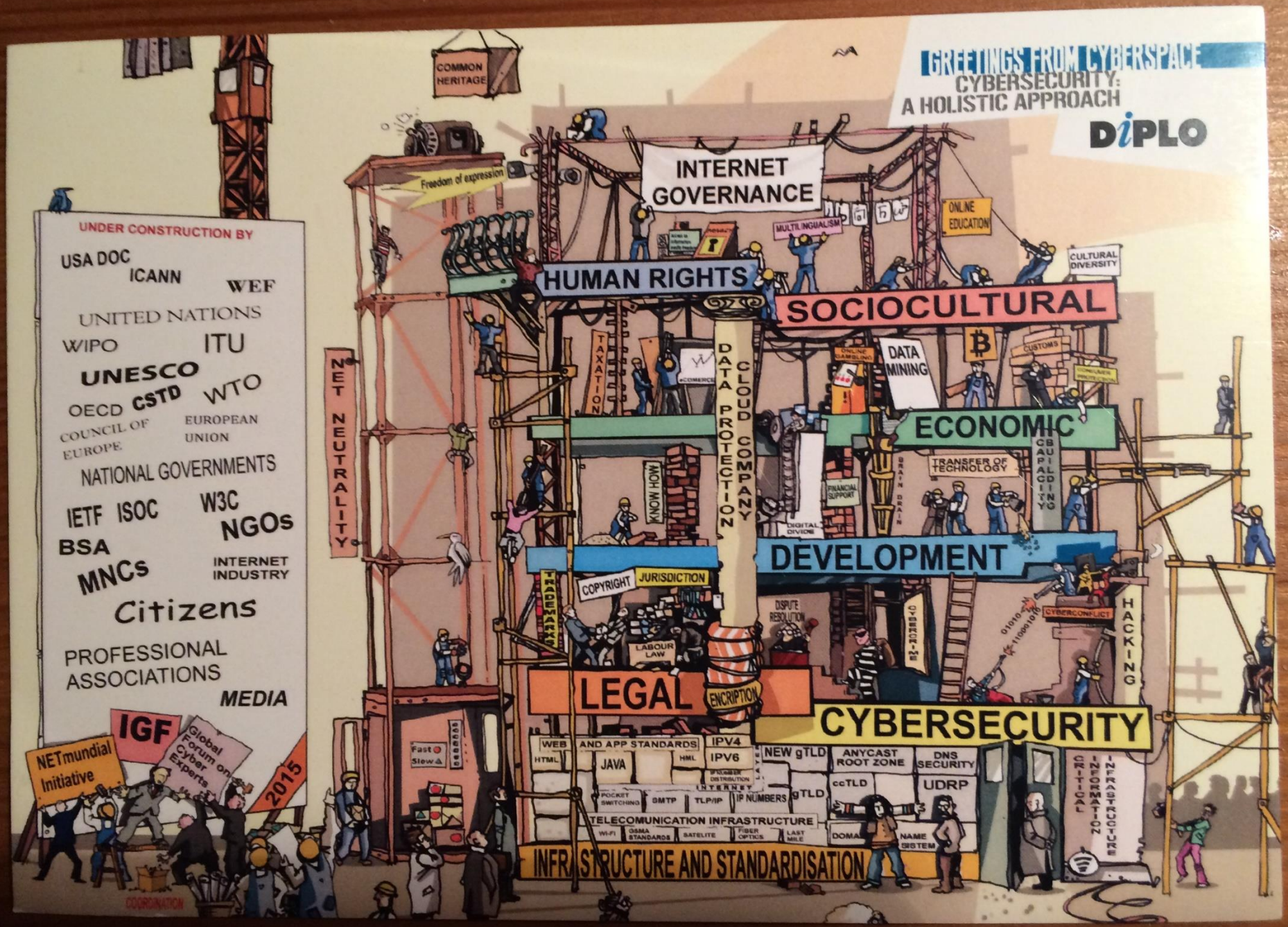
CYBERDIPLOMACY

EU Study Week

Autumn 2020

Marina Kaljurand

"On the Internet, nobody knows you're a dog."


GREETINGS FROM CYBERSPACE
CYBERSECURITY:
A HOLISTIC APPROACH
DiPLO
UNDER CONSTRUCTION BY
USA DOC
ICANN
WEF
UNITED NATIONS
WIPO
ITU
UNESCO
OECD
CSTD
WTO
COUNCIL OF EUROPE
EUROPEAN UNION
NATIONAL GOVERNMENTS
IETF
ISOC
W3C
NGOs
BSA
MNCs
INTERNET INDUSTRY
Citizens
PROFESSIONAL ASSOCIATIONS
MEDIA
IGF
NETmundial Initiative
Global Forum on Cyber Experts
2015
COORDINATION
COMMON HERITAGE
Freedom of expression
INTERNET GOVERNANCE
MULTILINGUALISM
ONLINE EDUCATION
CULTURAL DIVERSITY
HUMAN RIGHTS
SOCIOCULTURAL
NET NEUTRALITY
TAXATION
DATA PROTECTION
CLOUD COMPANY
DATA MINING
CUSTOMS
ECONOMIC
KNOW HOW
TRANSFER OF TECHNOLOGY
FINANCIAL SUPPORT
BRAIN DRAIN
CAPACITY BUILDING
DIGITAL DIVIDE
DEVELOPMENT
COPYRIGHT
JURISDICTION
TRADEMARK
DISPUTE RESOLUTION
CYBERCRIME
CYBERCONFLICT
HACKING
LABOUR LAW
LEGAL
ENCRIPTION
CYBERSECURITY
WEB
AND APP STANDARDS
IPV4
IPV6
HTML
JAVA
XML
NEW gTLD
ANYCAST ROOT ZONE
DNS SECURITY
ccTLD
UDRP
gTLD
POCKET SWITCHING
SMTP
TLP/IP
IP NUMBERS
TELECOMUNICATION INFRASTRUCTURE
WI-FI
GSMA STANDARDS
SATELITE
FIBER OPTICS
LAST MILE
DOMAIN NAME SYSTEM
CRITICAL INFORMATION INFRASTRUCTURE
INFRASTRUCTURE AND STANDARDISATION

1. WB Report: Digital Dividends

2. Case of Estonia: impact of the use of ICTs. Lessons learned from 2007

3. Existing and emerging threats. Hacking Democracy: US elections (2016)

4. International cooperation (UN, OSCE, NATO, EU)

5. International law

6. Multistakeholder model: Paris Call

7. Information operations. Fake news. EU response

8. EU East StratCom Task Force

World Development Report: Digital Dividends

- Greatest ICT revolution in human history
- 40% of world`s population has access to the internet
- 20% of poorest households are more likely to have better access to mobile phones than to toilets and clean water
- Use of ICTs create new opportunities, but also challenges
- New opportunities through inclusion, efficiency, innovation
- Nearly 6 billion people do not have high-speed Internet, so they can`t fully participate in the digital economy

Impact of ICTs

- **Governance**: open, transparent, participation of citizens
- **Economy**: digitalization increases productivity, spurs innovation; most successful are the businesses that are innovative and invest in RD
- **PPP**: private sector owns critical infrastructure, provides e-services, solutions for secure data exchange, integrity of data
- **Civil Society**: Let`s do it
- **Democracy**: human rights, internet freedom, gender equality.

Impact of COVID-19

- Benefits
- Challenges

Case study: Estonia

- 84% of population of age 16-74 uses internet
- 83% of households have internet capabilities
- 98% of households with children have internet capabilities
- All schools, libraries, public buildings have free WIFI
- Digital signature: 900+ million given; save 2% of GDP = 5 working days
- Online voting: from 2% in 2005 to 30% in 2015; 2019 – 46% (EP)
- Mark Zukerberg (Harvard Commencement speech 2017): modernize democracy so that everyone can vote online
- E-residents: annually 14-15 000 new e-residents; 5000 companies established by e-residents

E- residency


DIGITAALNE ISIKUTUNNISTUS
DIGITAL IDENTITY CARD
LUCAS
EDWARD
30.11.2017
N0100001
36205030034
AINULT ELEKTROONILISEKS KASUTAMISEKS
ELECTRONIC USE ONLY

Let's do it!

Let`s do it

- Global civic movement with a mission to connect and empower people and organizations around the world to make our planet waste free
- 03.05.2008 – 1st clean up day in Estonia: 50 000 persons cleaned up 10 000 tons of garbage in 5 hours
- 2012 – 96 countries participate in 1st world clean up day (6,3 millions)
- 2014 – 12,2 millions; decided to launch new initiative
- **world clean up day** on 15.09.2018: 150 countries and 50 million tons

2007 – lessons learned

- Importance of political decision making – high on political agenda, including financing
- Have house in order – legal frameworks, strategies, clear division of responsibilities, accountability
- All-nation approach – coopeation with private sector, academia, civil society, IT folks/community
- Public-private-partnership
- International cooperation

International cooperation – UN

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

Mandate:

1. new/emerging threats
2. applicability of international law
3. norms (non-binding) of responsible state behavior
4. confidence building measures
5. capacity building measures

Applicability of International Law

- 2013, 2015: International Law (IL), in partcular UN Charter in its entirety applies to the use of ICTs
- HOW IL applies to cyber?
- Existing IL *versus* writing new IL : Code of Conduct; Geneva Digital Convention
- Tallinn Manual 2.0 on application of IL (2016)
- „Grey zones“ of IL, e.g. responsibilty of states for the acts of non-state actors; violation of sovereignty and territorial integrity; protection of critical infra

International cooperation - OSCE

2016 – Second Set of Cybersecurity Confidence Building Mesures; 2017 – failed to make progress

Objective – build confidence, avoid escalations, mistakes

- sharing information
- opening lines of communication
- facilitating cooperation
- fostering understanding
- protecting critical infrastructure
- responding to threats

International cooperation - NATO

- responsibility of NATO is to defend its own networks
- responsibility of Allies is to develop the relevant capabilities for the protection of national networks
- Article 5 - North Atlantic Council (political) decision, case-by-case
- planning, training, education, exercises
- cyber - 5th domain of operations
- national cyber commands – USA, UK, NL, DE, FR. EE – fully operational in 2020
- NATO CCD COE

International cooperation - EU

- Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities – Cyber Diplomacy Toolbox
- Joint EU diplomatic response to malicious cyber activities
- Joint measures within the CFSP include restrictive measures, adopted under the relevant provisions of the Treaties
- Follow main principles, including serve to protect the integrity and security of the EU, its MS and their citizens

What states can do and have done
State practice

- Importance of states' practice
- 2015 – US attributed cyber attacks against Sony to North Korea and introduced countermeasures
- 2016 – US attributed DNC hacks to Russia and introduced countermeasures (expelled diplomats)
- 2017 – US attributed *WannaCry* to North Korea
- 2017 – UA attributed attacks against CI/power grid to Russia, after US DoS did it.

Multistakeholder Approach to Cybersecurity

- Industry/Private Sector (Microsoft; Siemens)
- Civil Society (GCSC; Carnegie)
- Academia (Tallinn Manual)
- IT experts/organizations (ISOC standards)

Paris Call for Trust and Security in Cyberspace

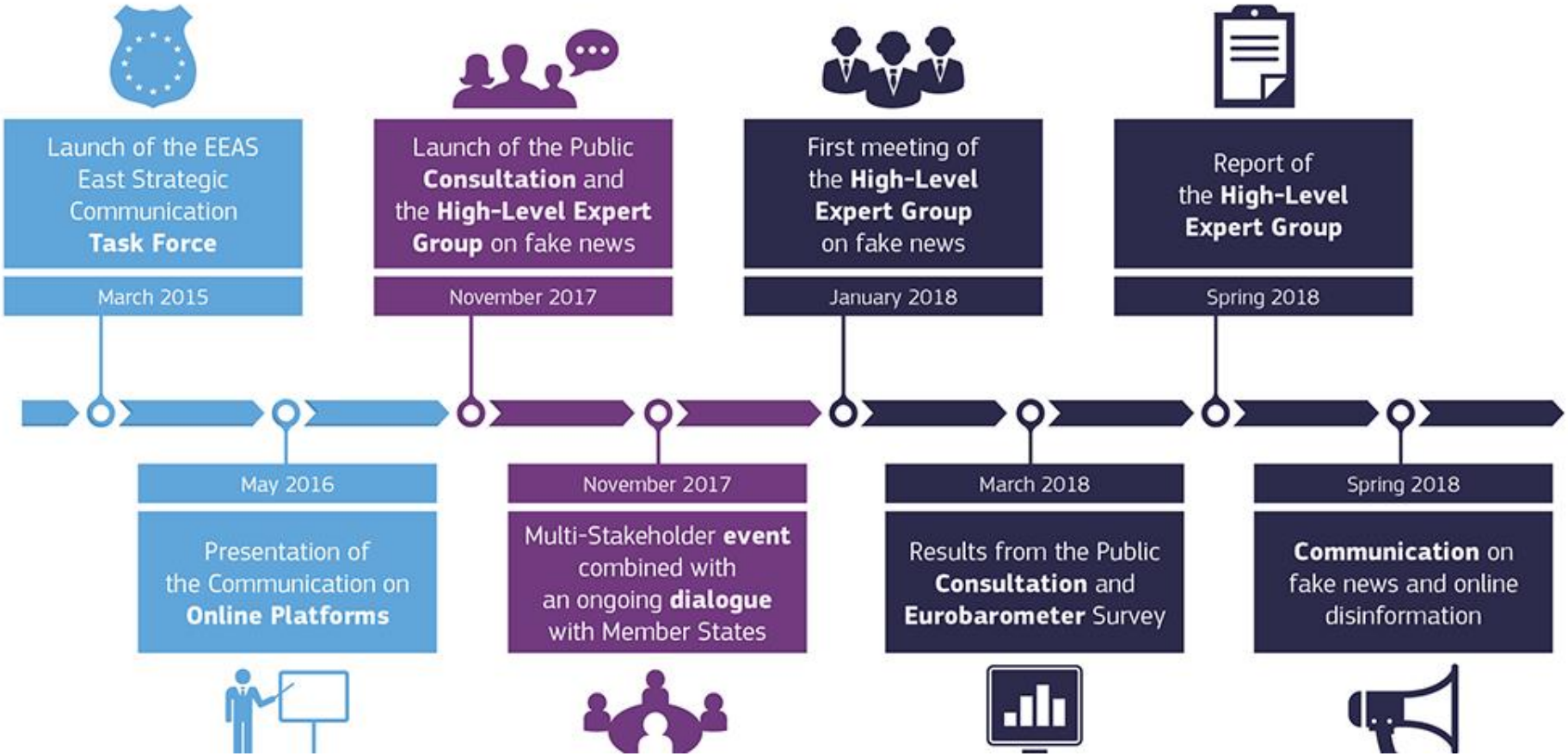
- Launched by President Macrone on November 12, 2018
- Reiterates what has been agreed internationally – e.g. applicability of IL
- Introduces norms of responsible state behaviour
- Multistakeholder approach
- Follow-up meeting in 2019
- Follow-up and role of IGF (Internet Governance Forum)


WANTED
the ambassador
of the fascist
state

Joseph S. Nye: Information Warfare *versus* Soft Power; Project Syndicate
https://www.project-syndicate.org/commentary/cyber-warfare-weakens-russia-soft-power-by-joseph-s--nye-2017-05?barrier=accesspaylog

- Putin (2012): "Soft power is a complex of tools and methods to achieve foreign policy goals without the use of force, through **information and other means of influence.**"
- soft power **is not any action** other than military force.
- soft power is the ability to get what you want through **attraction and persuasion** rather than threats of coercion or offers of payment
- soft power is nor good or bad in itself. Value judgements depend on the ends, means, and consequence of an action.
- soft power is a battle for hearts and minds (VoA, Marshall Plan)
- Information warfare – "negative soft power"
- 19th century – whose army won; today – whose story wins

Tackling Fake News in the EU



Action Plan against Disinformation

- 83% of Europeans think fake news is a threat to democracy
- 73% of internet users are concerned about disinformation online in the EP pre-election period
- Action Plan answers the European Council's call for measures to "**protect the Union's democratic systems and combat disinformation, including in the context of the upcoming European elections**"
- It builds on existing Commission initiatives and the work of the East Strategic Communication Task Force of the European External Action Service

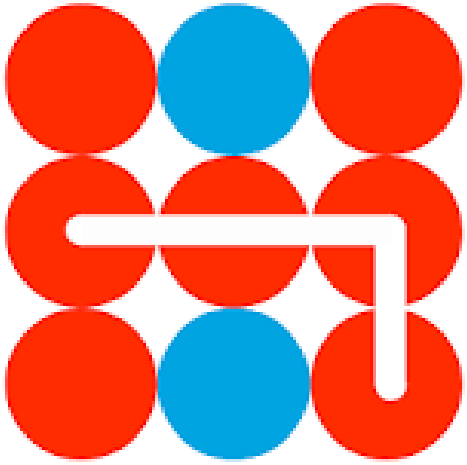
East StratCom Task Force

- under High Representative/Vice-President Mogherini
- set up in March 2015, for countering disinformation in the EU's Eastern Neighbourhood
- team of 14 Russian-language and communications specialists, EE seconded 1 expert
- produces **Disinformation Review** which focuses on key messages carried in the international information space, which have been identified as providing a **partial, distorted or false view or interpretation and/or spreading key pro-Kremlin messaging**

NATO Strategic Communications CoE, Riga

- **Contribute** positively and directly in achieving the successful implementation of NATO operations, missions, and activities by incorporating strategic communications planning into all operational and policy planning
- Build, in close and lasting coordination with NATO nations, **public awareness**, understanding, and support for specific NATO policies, operations, and other activities in all relevant audiences
- Contribute to **general public awareness** and understanding of NATO as part of a broader and on-going public diplomacy effort

European CoE for Countering Hybrid Threats, Helsinki



- joint project of the EU and NATO
- a hub of expertise supporting the participating countries' individual and collective efforts to enhance their civil-military capabilities, resilience, and preparedness to counter hybrid threats with a special focus on European security

Thank you!