Dutch Cyber Landscape

Policy, organisation, issues

Embassy of the Kingdom of the Netherlands in Rome

Agenda

- Cybersecurity all around us: opportunities and challenges
- Dutch cyber security policy, priorities and organization
- Cybersecurity in international relations
- Dilemmas
- Q&A

Cyber: Opportunities and Challenges

Dutch media outlets take EU to court over disinformation claims

'Godkiller' and 'Atreexp': the Chinese hackers accused of global attacks

The pair are alleged to be part of group that has been infiltrating computers systems since 2006

11:02 / 28.06.2018   **To russian version**

Russian activists turn to UN Human Rights Council about Internet censure

Facebook fake news inquiry: the countries demanding answers

NEWS

How the Dutch foiled Russian 'cyber-attack' on OPCW

🕐 4 October 2018

Cyber risk is evolving at unprecedented speed, and many businesses are ill-prepared

Vertaal Tweet

Uncharted territory: preparing for the unknown

Vietnam's new Cybersecurity Law could further undermine free speech and disrupt businesses
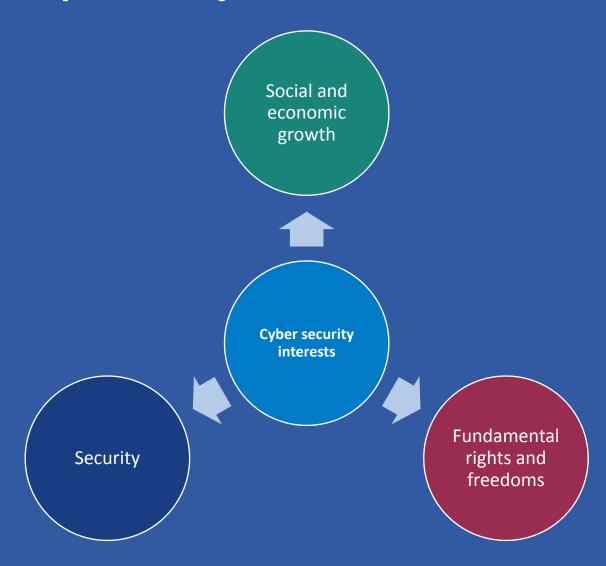
Avaaz ✓ @Avaaz
New @Avaaz study shows: EU elections under massive #disinfo threat. 100 mio views on Yellow vest fake news. @POLITICOEurope -- it's high time for @JKingEU @GabrielMariya @Ansip_EU @JunckerEU @VeraJourova to get much more serious abt this! politico.eu/article/yellow... @PoliticoRyan

Study: Yellow Jackets 'fake news' shared millions of ti...
politico.eu

Conflicting or complementary fundamental interests?

Challenge 1: security vs. privacy

Challenge 2: new technologies

Challenge 3: Geopolitical developments

The New York Times

In 5G Race With China, U.S. Pushes Allies to Fight Huawei

The Dutch Approach
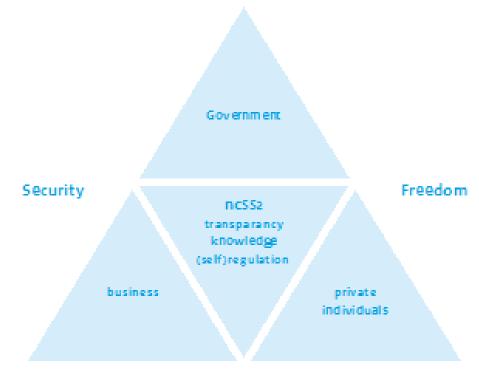
Vision statement

Together with the private sector, the technology community, academia and non-government organisations (NGOs), the Dutch government is committed to ensuring:

a safe, free and open digital domain, in which we can confront threats, protect fundamental rights and values, and take full advantage of the opportunities that digitalisation offers our society.

The Dutch Approach: Multistakeholder model

Policy priorities

Various policy documents inform the Dutch cyber security strategy.

Broader policy:
- Economic growth & sustainable d... ...f the intern...
- Effective internet gov...
- Further enhancement ...rity
- Effective ...to... ...e...
- Interna... ...ecurity and...
- Rights a... ...ee...

Digitization Strategy

Dutch Cyber Security Agenda

Defence White Paper

Broad Agenda Digital Government

Integrated International Security Strategy

Decentralised organisation

Cyber diplomacy at Ministry of Foreign Affairs

Three policy priorities
- Protect and strengthen international rule of law in cyberspace
- Human rights
- Capacity building
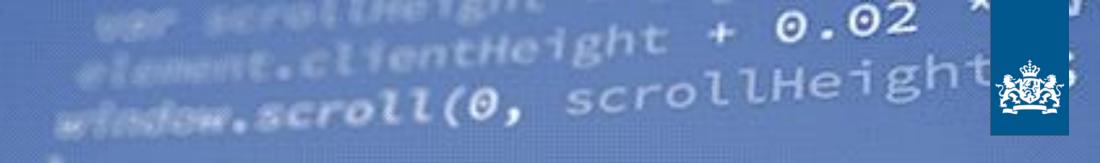
Security Department - Cyber Task Force

2020: EUR 2 mln annually for cyber diplomacy

Role for Embassy

- Develop a cybersecurity (multi-annual) plan
- Sketch cyber landscape in host country
- Ad hoc/structural outreach ahead of international conferences and/or demarches
- Proactive reporting about important cybersecurity developments, incidents, challenges

International peace and security

Normative framework

Rules of the cyber road: UN

- **Problem:**
  - Missing universal acceptance & application international law and additional, non-binding UN-norms

- **Strong divisions between countries to the cyber domain**:
  - Differences of opinion on the application of international law, norms of behavior in cyberspace and the dependence on and access to digital resources.

UN Processes

- Development normative framework came to a halt in 2017.
- In 2018 UNGA passed two competing resolutions, creating two parallel UN processes:
  - Proposal US for a new 6th, UN group of governmental experts (GGE);
  - Proposal RF c.s. for Open Ended Working Group (OEWG).

- Differences
  - GGE incremental process, continuation of previous GGE reports, 1 year
  - OEWG more open and consensus: continue work of GGE or foucs on crafting new (binding) instrument/treaty.

Rules of cyber: EU

- Existing cyber diplomacy toolbox for response measures and instruments

- OPCW hack led to discussions about a thematic EU cyber **sanctions** regime.
- Few difficulties
- Coordinated EU attribution

Diplomatic Response Framework

- Ministry of Foreign Affairs established assessment framework for diplomatic responses
- Reasons: cyber incident, request partner country, participating in coalition EU/NATO
- Integral and adequate consideration of interests: geopolitical interests, information position, research interests, possible consequences for national security.
- Escalation ladder of response measures

Attribution

- <u>3 types of attribution</u>
  - technical (services)
  - political (action)
  - legal (international law)

- <u>Objectives of attribution</u>
  - Deterrence
  - Building precedents and norms
  - Visibility public

Examples of public attributions

- December 2016: US attributes '**DNC hack**' to Russia.
- December 2017: US with Five-Eyes and Denmark '**WannaCry**' to DPRK.
- February 2018: Five-Eyes and few EUMS '**NotPetya**' to Russia.
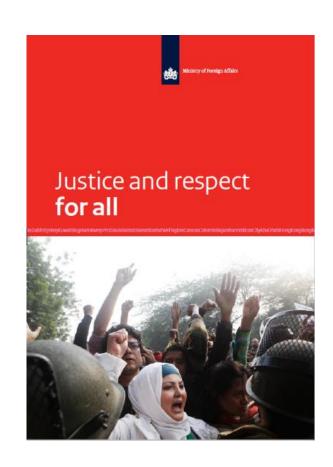- October 2018: NL reveals Russian cyber operation against **OPCW** in press conference

Ministry of Foreign Affairs

Human Rights Online

1-5-2019

Policy framework

Human Rights on the Internet

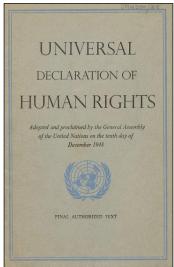1 of 6 priorities in human rights policy (DMM-MP)

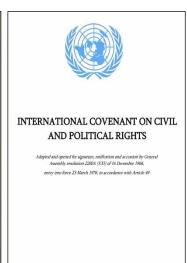1 of the pillars of cyber policy (DVB-TFCYBER)

International norms and convenings

Offline = online

FOC: fou

Current FOC member states

FREEDOM ONLINE COALITION

FOC – MEMBERSHIP GROWTH

2011	2011/12	2012/13	2013/14	2014/15	2015/16
13	+5	+3	+2	+4	+3
Austria	Costa Rica	Georgia	Japan	Australia	New Zealand
Canada	Finland	Germany	Moldova	Lithuania	Spain
Czech Republic	Ghana	Latvia		Norway	Argentina
Estonia	Mexico			Poland	
France	Tunisia				
Ireland					
Kenya					
Mexico					
Mongolia					
Netherlands					
Sweden					
UK					
USA					

Possible new members 2018-2019:
Belgium, Luxemburg, Uruguay

Programs supported by MFA

Digital Safety Manual: Protecting human rights online in practice

Local organisations & projects

Capacity Building
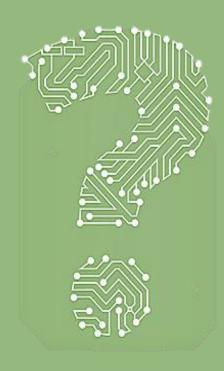
Thank you for your attention

Follow us:

Olandiamo.in.italia

@Olandiamo
@dewivandeweerd
@jdsaman

Olandiamo