RIPE

Cybersecurity Due Diligence

an ISP Perspective

Joanna Kulesza, October 27th, 2016

New challenges, old solutions?

Let’s start with some examples

Joanna Kulesza, October 27th, 2016

World news

Russia accused of unleashing cyberwar to disable Estonia

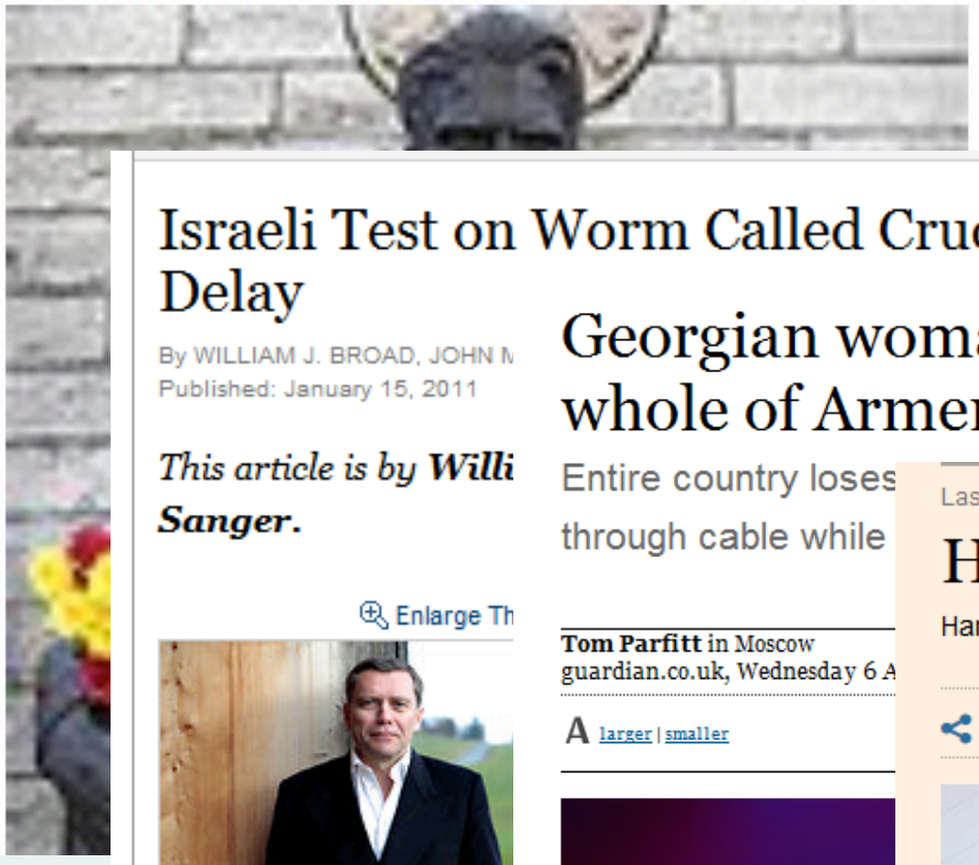
- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences

Ian Traynor in Brussels

Thursday 17 May 2007 02.32 BST

This article is 8 years old

Save for later



Israeli Test on Worm Called Crucial in Iran Nuclear Delay

By WILLIAM J. BROAD, JOHN M
Published: January 15, 2011

*This article is by **Willi Sanger**.*

Enlarge Th

Nicholas Roberts for The New Y

Ralph Langner, an independent computer security expert, solve Stuxnet.

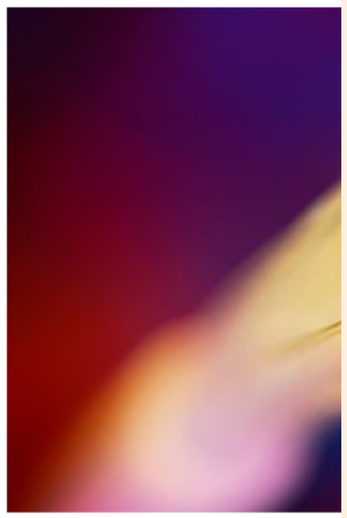
Multimedia

Georgian woman cuts off web access to whole of Armenia

Entire country loses through cable while

Tom Parfitt in Moscow
guardian.co.uk, Wednesday 6 A

A larger | smaller



The woman damaged a fibre-opt

An elderly Georgian woma accidentally sliced through neighbouring Armenia, it e

The woman, 75, had been

Last updated: January 5, 2016 10:37 pm

Hackers shut down Ukraine power grid

Hannah Kuchler in San Francisco and Neil Buckley in London

Share | Author alerts | Print | Clip | Comments

Hackers brought down the power supply to hundreds of thousands of homes in Ukraine last week, in a cyber attack believed to be the first ever to result in a power outage.

The Ukrainian energy ministry said it was probing a "suspected" cyber attack on the

Joanna Kulesza, October 27th, 2016

Cybersecurity challenge

- potential **targets** of cyberthreats?

- infrastructure and systems the malfunction of which imminently results in "**significant**" damage or puts a large number of individuals at risk

- civil defense notion of "**critical infrastructure**" (means of mass transportation, water, or electricity supplies and the like)

Council Directive 2008/114/EC
of 8 December 2008

on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (ECIs)

OJ L 345, 23.12.2008, p. 75–82

provides guidelines on identifying elements of critical infrastructure and setting particular obligations on its operators, including running a **risk analysis** for those particularly vulnerable assets

sets **obligations** to provide the maximum level of security and resiliency of systems crucial for European security

Joanna Kulesza, October 27th, 2016

Legal notice | Contact | Search English (en)

European Commission

EUROPEAN COMMISSION

ERNCIP Inventory

European Commission > JRC Hub > ERNCIP Inventory

erncip

project platform

European Reference Network for Critical Infrastructure Protection

The ERNCIP Inventory is a free-to-use search tool for open-source information on European security experimental and testing facilities. The system stores detailed profiles of laboratories which have capabilities in the field of Critical Infrastructure Protection.

The ERNCIP Inventory is open to searching by any stakeholder interested in Critical Infrastructure Protection, such as:

- ✔ Governments
- ✔ Critical Infrastructure Operators
- ✔ Research Centers
- ✔ Universities
- ✔ Manufacturers

who could use it to find solutions to security problems, business partners, contractors, or consultancy.

Access for Searching

E-mail

name@domain.com

F97GBW

RIPE

The ERNCIP Project Platform

Our mission is to foster the emergence of **innovative**, **qualified**, **efficient** and **competitive security solutions**, through the networking of European **experimental capabilities**.

TG - Thematic Groups

- Applied Biometrics for Critical Infrastructure Protection
- Aviation Security Detection Equipment
- Chemical and Biological (CB) Risks to Drinking Water
- Detection of Explosives & Weapons at Secure Locations
- Detection of Indoor Airborne Chemical-Biological Agents (New)
- Radiological and Nuclear Threats to Critical Infrastructure

Upcoming events

Radiological and Nuclear threats to critical infrastructure TG Meeting (Coordinator and Lead Scientists)
Thu Mar 17, 2016 @ 9:00AM
JRC Ispra (Italy)

Radiological and Nuclear threats to critical infrastructure TG Meeting (Coordinator and Lead Scientists)
Fri Mar 18, 2016 @ 9:00AM
JRC Ispra (Italy)

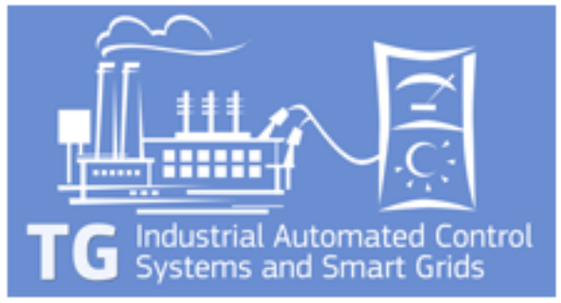
Detection of Indoor Airborne Chemical-Biological Agents TG Meeting
Fri Apr 01, 2016 @ 8:00AM

Latest deliverables

ERNCIP-Newsletter-No15
31 Tuesday, 16 February 2016 10:38
Download

Recommendations for the improvement of existing European norms for testing the resistance of windows and glazed façades to explosive effects
31 Thursday, 03 December 2015 12:40
Download

ERNCIP-Newsletter-No14
31 Friday, 09 October 2015 08:43
Download



Industrial Automated Control Systems and Smart Grids IACS & SG

Challenge

Information and Communication Technology (ICT) is becoming more and more important in the delivery of essential services. Recent incidents have shown that Industrial Automation and Control Systems (IACS) can be vulnerable to cyber attacks and that such attacks can lead to disruptions of physical systems and networks. This makes security for IACS an important part of Critical Information Infrastructure Protection (CIIP).

Focus of work

The Thematic Group considered the common definitions for IACS, Smart Grids, and on whether to test at component or system level. With diverse views provided from the group, consensus proved difficult to achieve on the scope of the work streams that the TG will undertake. Options are for the TG to focus on the human vulnerabilities of IACS systems, and to investigate the need for work on testing and certification of technology components.

Outcome

This Group ceased in 2013, after contributing to the Global Information Assurance Certification (GIAC) initiative that led to the launching of the vendor-neutral Global Industrial Cyber Security

Upcoming events

No events

Latest News

6th and 7th Industrial Automated Control Systems (IACS) and Smart Grids TG meeting

2013-Jun-14

Tele-conference on 3 June and meeting on 14 June 2013, JRC Ispra The Trusted Test Centres for IACS...

5th meeting of Industrial Automation and Control Systems (IACS) TG

2013-Feb-01

I

(Legislative acts)

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 6 July 2016

concerning measures for a high common level of security of network and information systems across the Union

Network and Information Security Directive: co-legislators agree on the first EU-wide legislation on cybersecurity

Published on 09/12/2015

On 7th December 2015, the European Parliament and the Council reached an agreement on the Commission's proposed measures to increase online security in the EU. The Network and Information Security (NIS) Directive is the first piece of European legislation on cybersecurity. Its provisions aim to make the online environment more trustworthy and, thus, to support the smooth functioning of the EU Digital Single Market.

The proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union was put forward by the European Commission in 2013. Two years later, the Parliament and the Council have agreed on a set of measures to boost the overall level of cybersecurity in the EU.

The new rules will:

- improve cybersecurity **capabilities** in Member States
- improve Member States' **cooperation** on cybersecurity
- require **operators of essential services** in the energy, transport, banking and healthcare sectors, and providers of key digital services like search engines and cloud computing, **to take appropriate security measures and report incidents to the national authorities**.

Following this political agreement, the text will have to be formally approved by the

DIRECTIVE 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning measures for a high common level of security of network and information systems across the Union

ANNEX II (essential services)

1. Energy (a) Electricity; (b) Oil; (c) Gas
2. Transport (a) Air transport; (b) Rail transport; (c) Water transport; (d) Road transport
3. Banking
4. Financial market in-frastructures
5. Health sector
6. ~~Drinking water supply and~~ distribution
7. **Digital Infrastructure: IXPs; DNS service providers; TLD name registries**

DIRECTIVE 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning measures for a high common level of security of network and information systems across the Union

Annex III

ANNEX III TYPES OF DIGITAL SERVICES FOR THE PURPOSES OF POINT (5) OF ARTICLE 4

1.Online marketplace.

2.Online search engine.

3.Cloud computing service.

Joanna Kulesza, October 27th, 2016

DIRECTIVE 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

concerning measures for a high common level of security of network and information systems across the Union

key challenges:

- identifying critical infrastructure (a shared definition?)

- individual obligations of CI operators

- financial support for additional security measures

- exchange of information (scope, platform)

The principle of due diligence in international law

- a subsidiary principle of the law on state responsibility

ILC (2006): *The notion of "transboundary damage", like the notion of "transboundary harm", focuses on damage caused in the jurisdiction of one State by activities situated in another State. (…) the non-fulfilment of the duty of prevention (…) could engage State responsibility without necessarily giving rise to the implication that the activity itself is prohibited*

- applicable to obligations of conduct (not ones of result)
- assesment based on state efforts to prevent significant transboundary harm („all neccesary measures")

significant transboundary harm in international law

state responsibility applicable only in cases of „significant" harm, i.e.

ILC (2006): The term "significant" is understood to refer to something more than "detectable" but need not be at the level of "serious" or "substantial".

ILC (2001): The term "significant", while determined by factual and objective criteria, also involves a value determination which depends on the circumstances of a particular case and the period in which such determination is made.

Duty of prevention

- The risk of significant transboundary harm originates a state duty of prevention
- a best efforts obligation to prevent such harm
- Individual treaty regimes specify details of this obligation in paricular circumstances (e.g. environmental law, law of treaties, protection of aliens, space law, antiterrorist treaties)

International treaty practice

Usual references to:

- „best available technologies” or
- „newest technological developments”

ILC (2006): The State of origin is expected to perform the obligation of due diligence both at the stage of authorization of hazardous activities and in monitoring the activities in progress after authorization and extending into the phase when damage might actually materialize, in spite of best efforts to prevent the same. (…)

Further, the State concerned should ever be vigilant and ready to prevent the damage as far as possible and when damage indeed occurs to mitigate the effects of damage with the best available technology

The principle of due diligence

1. Good faith
2. Good neighborliness
3. Limits of state jurisdiction
4. Sustainable development
5. The obligation to take all neccesary measures

a hypothetical model of a „good government”, expected to enforce apriopriate administrative and other procedures

The principle of due diligence

6. State efforts assessed against current technological advancements as well as individual economic and technological situtation of the state of origin

7. An obligation to exchange information

including consultations with potentially affected parties

8. No discrimination

9. A continuous obligation

a due diligence standard for cyberspace

Recommendation CM/Rec(2011)8

of the Committee of Ministers to member states on

the protection and promotion of the universality,

integrity and openness of the Internet

(Adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies)

Recommendation CM/ Rec(2011)8

Commitment to protect and promote the universality, integrity and openness of the Internet

1. General principles

1.1. No harm

1.1.1. States have the responsibility **to ensure**, (…)

1.1.2. (…), **that their actions within their jurisdictions do not illegitimately interfere with access to content outside their territorial boundaries or negatively impact the transboundary flow of Internet traffic.**

1.3. Due diligence

Within the limits of non-involvement in day-to-day technical and operational matters, states should, **in co-operation with each other and with all relevant stakeholders**, take all necessary measures to prevent, manage and respond to significant transboundary disruptions to, and interferences with, the infrastructure of the Internet, or, in any event, to minimise the risk and consequences arising from such events.

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

Note by the Secretary-General

The Secretary-General has the honour to transmit herewith the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The Group was established pursuant to paragraph 4 of General Assembly resolution 68/243.

Human rights due diligence

- The UN Protect Respect and Remedy Framework (Ruggie principles)

The Principles refer to three basic tools aimed at ascertaining human rights enforcement vis-a-vis transnational companies.

1) states' obligation to protect human rights,

2) corporate responsibility for their protection

3) accessibility of a legal remedy for victims of abuses caused by companies.

Contemporary international law does not permit putting international obligations directly onto private parties, therefore it is states who are obliged to assure that private companies operating under their jurisdiction, power or control meet human rights standards set by international law.

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

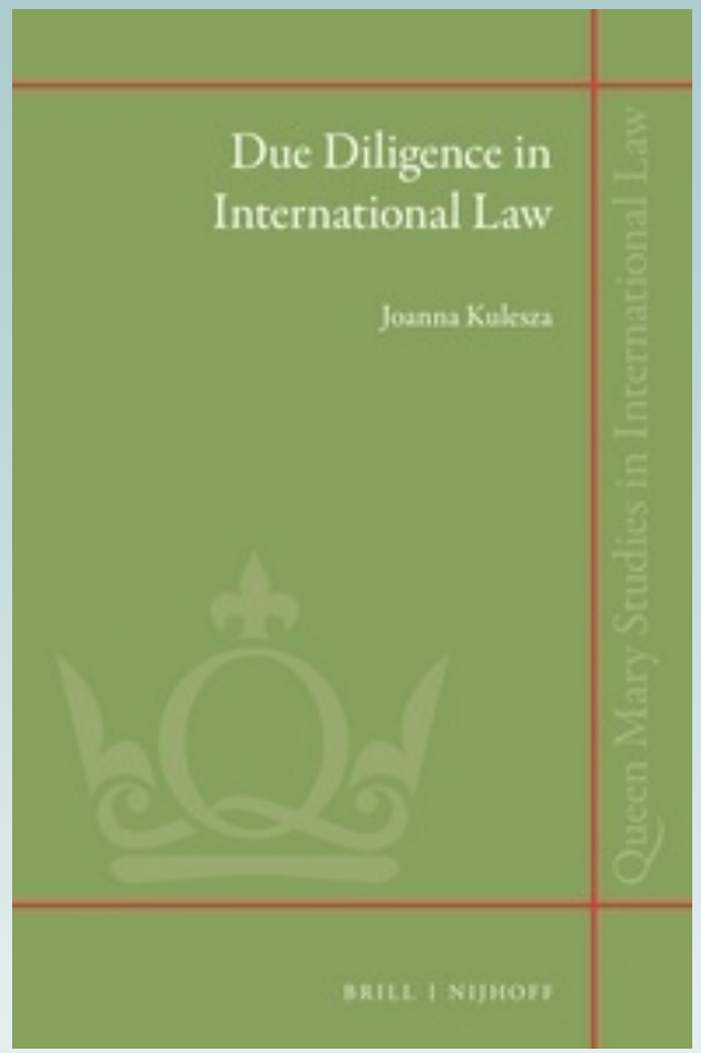
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

Questions to be considered

- Is there a due diligence standard for cybersecurity?
- Infrastrucutre operators liability? ISP liability fund?
- What are the consequences of the multistakeholder model?

RIPE



Thank you

joannnakulesza@gmail.com

RIPE

Questions?