Technische Hochschule
Brandenburg
University of
Applied Sciences
Institute for Security
and Safety

Evolving and Emerging Cyber Threats

WINS Workshop, Vienna

Guido Gluschke – March 19, 2017

Introduction

Guido Gluschke

Co-Director Institute for Security and Safety at the Brandenburg University of Applied Sciences

IAEA REGIONAL TRAINING COURSE ON
INFORM ON & COMPUTER SECURITY FOR
NUCLEAR URITY PRACTITIONERS, ACCRA-GHANA
DATE: 9th- DEC 2013
Venue: Gr ol of Nuclear ed Sciences Atomic Energy

Background:

- Computer Science / Cyber Security
- Security Management / Nuclear Security
- Critical Infrastructure Protection / Energy Sector

Program manager for joint activities with international organizations

Supporting International Initiatives On Cyber Security

UNODA United Nations Office for Disarmament Affairs

Groups of Governmental Experts (UN GGE)

"...examined the existing and potential threats from the cyber-sphere and possible cooperative measures to address them."

osce

OSCE Cyber Informal Working Group (OSCE IWG)

"... efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner in accordance with OSCE commitments and in co-operation with relevant international organizations..."

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENERGY

EU Energy Expert Cyber Security Platform - Expert Group (EECSP)

"The mission of the EECSP-Expert Group is to provide guidance to the Commission on policy and regulatory directions at European level, addressing the energy sector key points including infrastructural issues, security of supply, smart grids technologies as well as nuclear."

Supporting International Initiatives On Cyber Security

CPPNM and IAEA Nuclear Security Series (NSS)

"The amended Convention makes it legally binding for States Parties to protect nuclear facilities and material in peaceful domestic use, storage as well as transport."

NSS documents on computer security exists or are under development.

NTI Nuclear Cyber Security Expert Group

"Working with a global group of experts in nuclear engineering, cyber security, as well as regulators and technology developers on a set of forward-looking, ambitious principles or rules of the road for protecting nuclear facilities from cyber threats."

Chatham House Expert Group on Cyber Security in the Nuclear Sector

The goal of the project is to (1) assess the risks and vulnerabilities of the international civil nuclear sector in regards to cyber security and (2) identify potential policies and international measures to enhance cyber security in the wider nuclear security field.

US Energy Association

To improve cyber security situational awareness of Black Sea utilities and to enhance their ability to harden and make their networks more resilient in light of the growing regional cyber threat, the United States Energy Association (USEA) under its Energy Technology and Governance Program with USAID, organized the inaugural meeting of the Utility Cyber Security Initiative (UCSI) in Kiev

Outcome Of Past International Initiatives On Cyber Security ISS Was Involved In

Chatham House Report
Caroline Baylon with Roger Brunt and David Livingstone
Cyber Security at Civil Nuclear Facilities
Understanding the Risks

IAEA Nuclear Security Series No. 17
Technical Guidance
Reference Manual
Computer Security at Nuclear Facilities

OUTPACING CYBER THREATS
PRIORITIES FOR CYBERSECURITY AT NUCLEAR FACILITIES
NTI

NUCLEAR SECURITY
NS 22 Cyber Security for Nuclea
Security Professionals

ENERGY EXPERT CYBER SECURITY PLATFORM
Cyber Security in the Energy Sector
Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector
EECSP Report
February 2017

Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety
Cyber Security at Nuclear Facilities: National Approaches
An ISS Research Project in Cooperation with the Nuclear Threat Initiative (NTI)

Analysis of the Implementation of the Initial Set of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies
OSCE Organization for Security and Co-operation in Europe

IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities, IAEA Vienna, Mar 2011

NS 22 Computer Security for Nuclear Security Professionals, INSEN, Oct 2013

Cyber Security at Nuclear Facilities: National Approaches, Institute for Security and Safety, Potsdam, Jun 2015

Cyber Security at Civil Nuclear Facilities: Understanding the Risks, Chatham House, London, Oct 2015

Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities, Nuclear Threat Initiative, Washington, Dec 2016

Cyber Security in the Energy Sector - Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, European Commission, Brussels, Feb 2017

Analysis of the Implementation of the Initial Set of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, OSCE, Vienna, Feb 2017

CONTENT

Is The Cyber Threat Real For Nuclear?

Is Cyber An Evolving And Emerging Threat?

What Picture Gives Us A Good Understanding In Terms Of Cyber Defense?

Is A Full-scope Cyber Threat Assessment Possible?

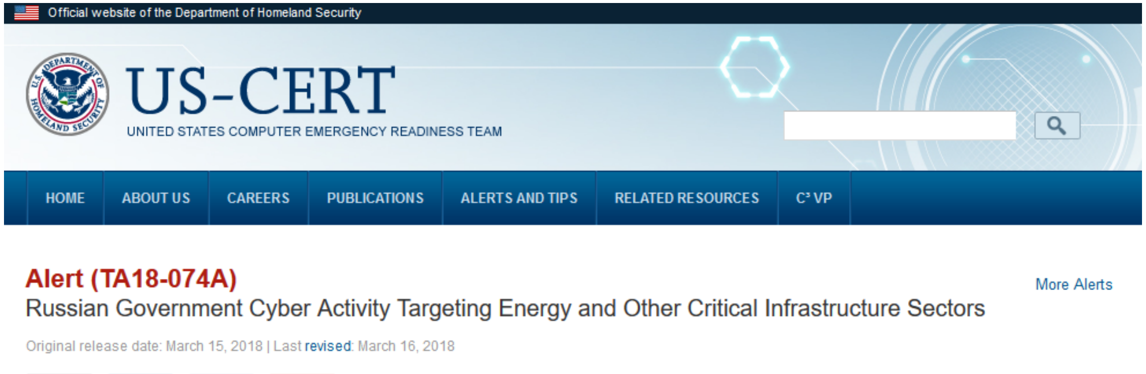
Are The Attributes And Characteristics From NSS10 (DBT) Applicable For Cyber?

Can We Keep Cyber Attacks Under Control?

What Is The Current Situation In Terms Of Cyber Threats?

What Are Examples For Future Cyber Threats?

Is The Cyber Threat Real For Nuclear?


Official website of the Department of Homeland Security
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
HOME
ABOUT US
CAREERS
PUBLICATIONS
ALERTS AND TIPS
RELATED RESOURCES
C³ VP
More Alerts

Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

Systems Affected

- Domain Controllers
- File Servers
- Email Servers

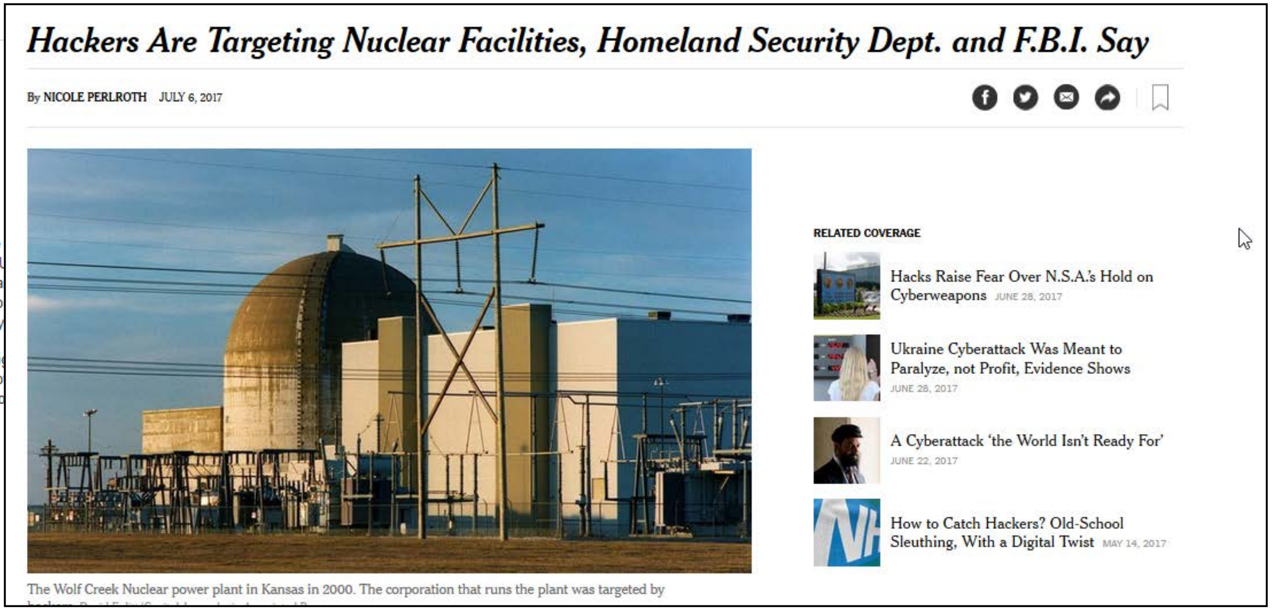
Overview

This joint Technical Alert (TA) is the result of analytic efforts between the
This alert provides information on Russian government actions targeting U
facilities, water, aviation, and critical manufacturing sectors. It also conta
procedures (TTPs) used by Russian government cyber actors on compro
enhance their ability to identify and reduce exposure to malicious activity

DHS and FBI characterize this activity as a multi-stage intrusion campai
where they staged malware, conducted spear phishing, and gained remo
cyber actors conducted network reconnaissance, moved laterally, and co

For a downloadable copy of IOC packages and associated files, see:

- TA18-074A_TLP_WHITE.csv
- TA18-074A_TLP_WHITE.stix.xml
- MIFR-10127623_TLP_WHITE.pdf
- MIFR-10127623_TLP_WHITE_stix.xml
- MIFR-10128327_TLP_WHITE.pdf
- MIFR-10128327_TLP_WHITE_stix.xml



Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say

By NICOLE PERLROTH JULY 6, 2017

RELATED COVERAGE

Hacks Raise Fear Over N.S.A.'s Hold on Cyberweapons JUNE 28, 2017

Ukraine Cyberattack Was Meant to Paralyze, not Profit, Evidence Shows JUNE 28, 2017

A Cyberattack 'the World Isn't Ready For' JUNE 22, 2017

How to Catch Hackers? Old-School Sleuthing, With a Digital Twist MAY 14, 2017

The Wolf Creek Nuclear power plant in Kansas in 2000. The corporation that runs the plant was targeted by

Source: https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html

Source: https://www.us-cert.gov/ncas/alerts/TA18-074A

Is The Cyber Threat Real For Nuclear?

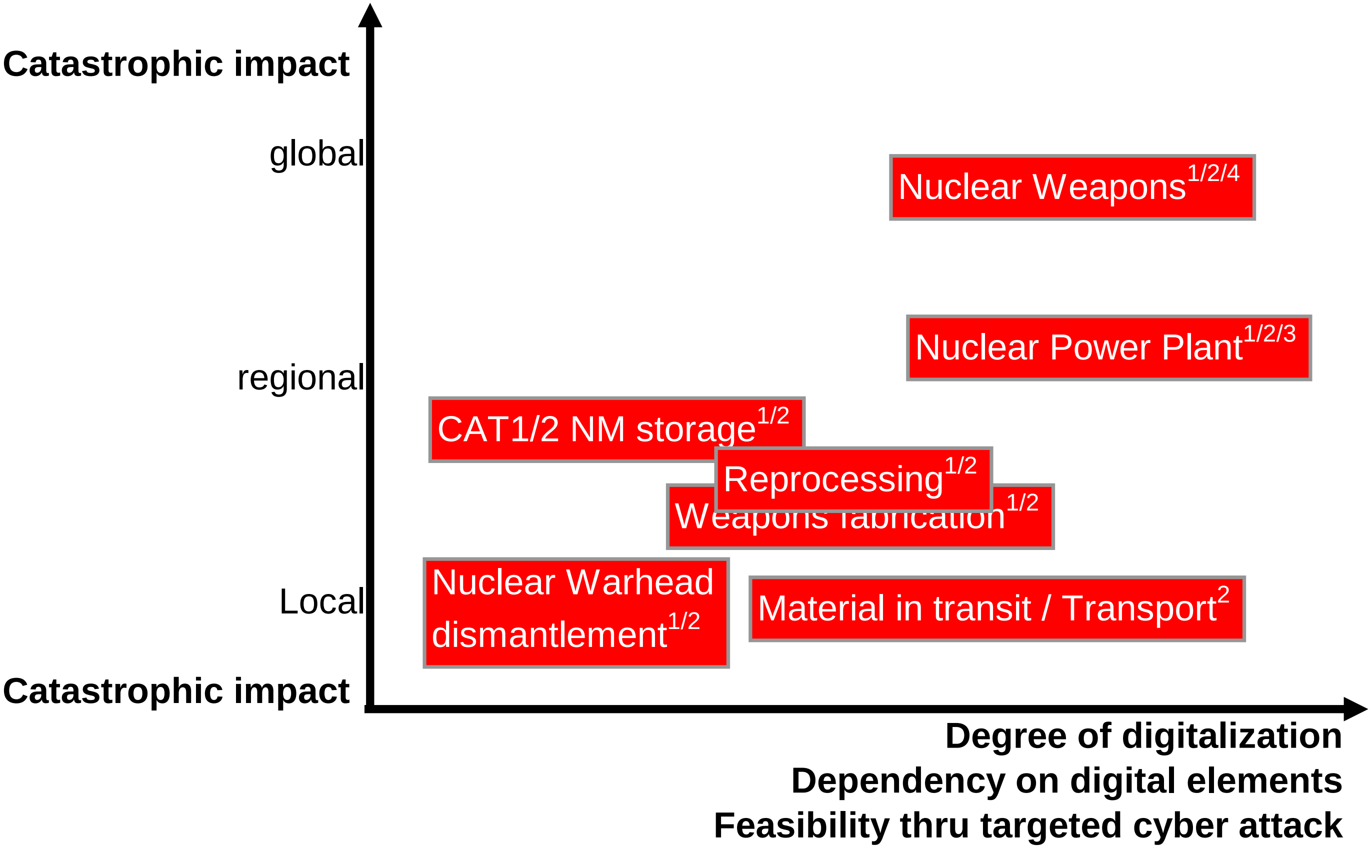
		Impact from		
		Unauthorized removal of material	sabotage of facility/equipment/ processes/material	theft of sensitive information
Nuclear Fuel Cycle	Mine or Mill			
	Conversion			
	Enrichment	unacceptable	unacceptable	unacceptable
	Fuel Fabrication	unacceptable	unacceptable	
	Research Reactor	unacceptable	unacceptable	
	Nuclear Power Plant	unacceptable	catastrophic	
	Spent Fuel Storage	unacceptable	unacceptable	
	Reprocessing	unacceptable	catastrophic	
	Disposal	unacceptable	unacceptable	
	Weapons Fabrication	unacceptable	catastrophic	unacceptable
Others	CAT1/2 NM storage	unacceptable	catastrophic	
	Radioactive sources		unacceptable	
	Nuclear weapons	unacceptable	catastrophic	unacceptable
	Dismantlement of nuclear warheads	unacceptable	catastrophic	unacceptable
	Safeguards / NMAC regime		unacceptable	unacceptable
	Material in transit / Transport (ground, air, water)	unacceptable	catastrophic	
	Border Monitoring / 2nd line of defense		unacceptable	unacceptable
	Electricity grids (impacting NPPs operations)		unacceptable	

Computer security incident which leads to an

unacceptable	event which could have a high impact and is in any case unacceptable for a nation state
catastrophic	event which could have a catastrophic impact for a nation state / int'l society / nuclear community

Source: G.Gluschke, ISS, April 2015

Is The Cyber Threat Real For Nuclear?



Catastrophic impact

global

regional

Local

Catastrophic impact

Nuclear Weapons[1/2/4]

Nuclear Power Plant[1/2/3]

CAT1/2 NM storage[1/2]

Reprocessing[1/2]

Weapons fabrication[1/2]

Nuclear Warhead dismantlement[1/2]

Material in transit / Transport[2]

Degree of digitalization
Dependency on digital elements
Feasibility thru targeted cyber attack

Worst case szenario

[1] Uncontrollable chain reaction

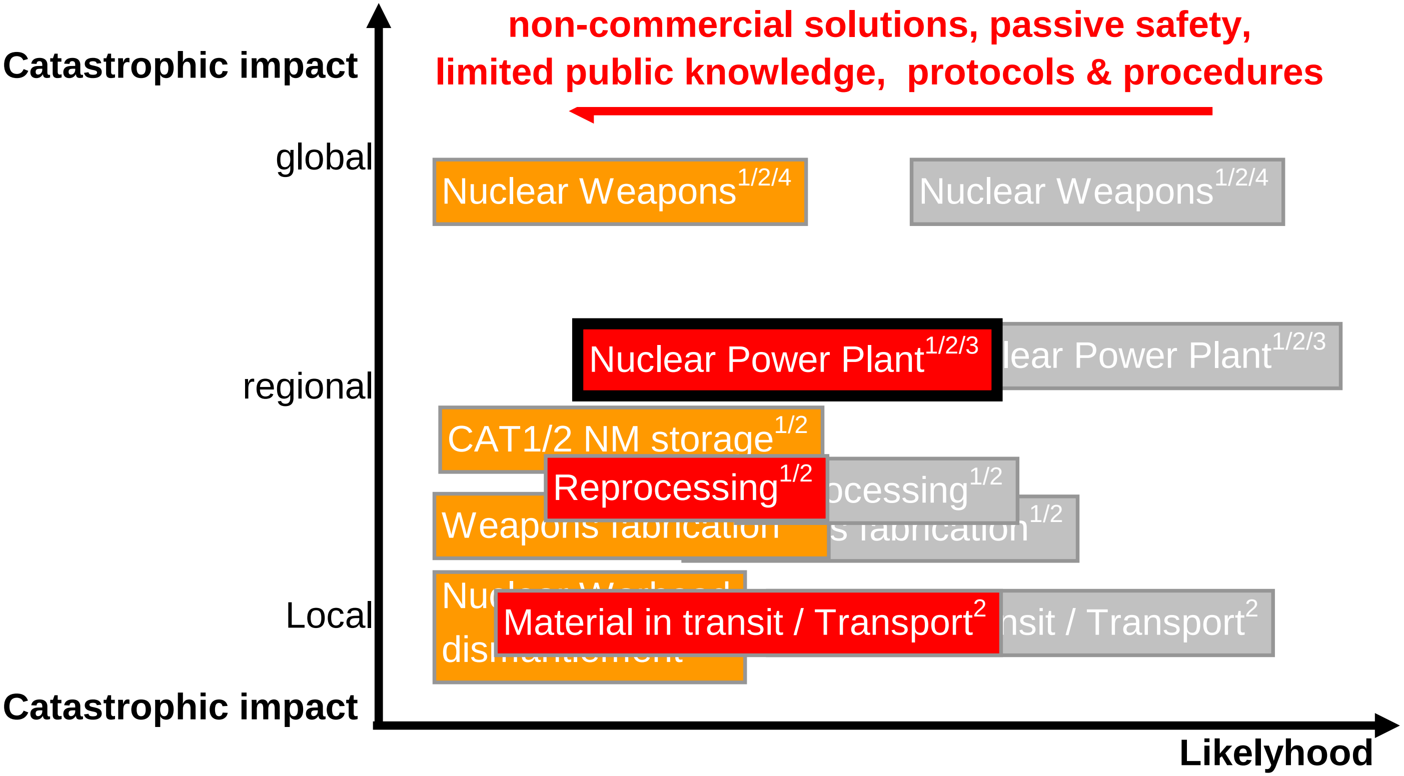
[2] Release of radioactive material

[3] (Long-term) outage of electricity grid

[4] Nuclear war

Source: G.Gluschke, ISS, April 2015

Is The Cyber Threat Real For Nuclear?



non-commercial solutions, passive safety,
limited public knowledge, protocols & procedures

Catastrophic impact

global

regional

Local

Catastrophic impact

Likelyhood

Nuclear Weapons[1/2/4]

Nuclear Weapons[1/2/4]

Nuclear Power Plant[1/2/3]

lear Power Plant[1/2/3]

CAT1/2 NM storage[1/2]

Reprocessing[1/2]

ocessing[1/2]

Weapons fabrication

s fabrication[1/2]

Nuclear Warhead dismantlement

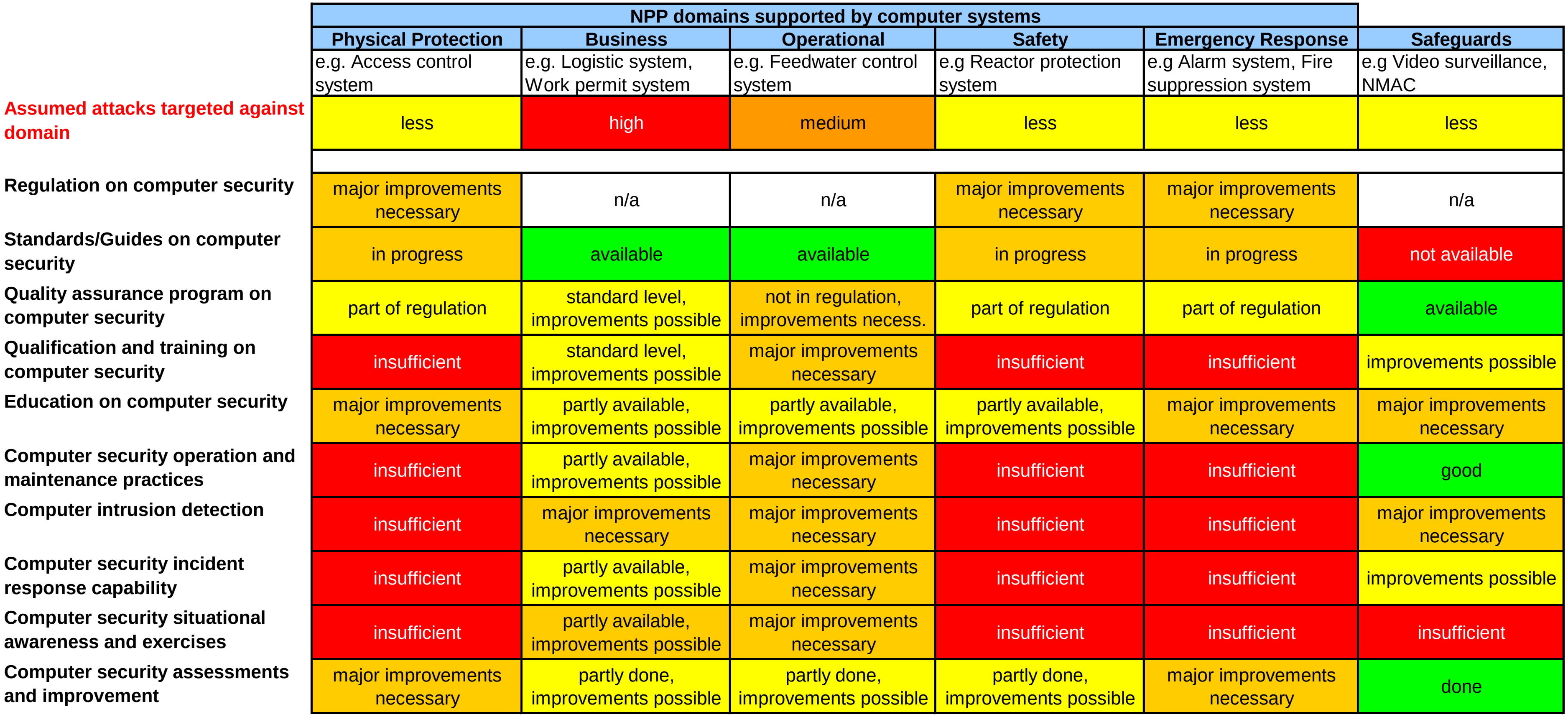
Material in transit / Transport[2]

nsit / Transport[2]

targeted attack against particular facility
or "target of oportunity" = more or less accident
(random target or proof of concept)

Source: G.Gluschke, ISS, April 2015

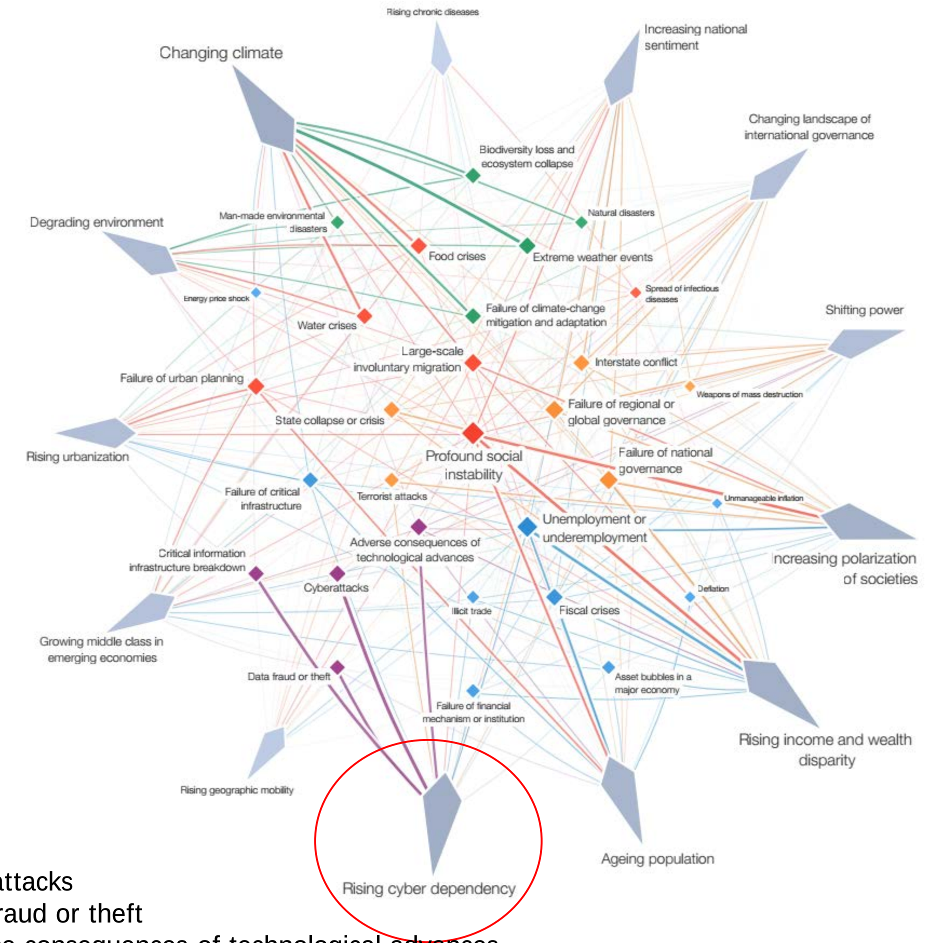
Is The Cyber Threat Real For Nuclear?

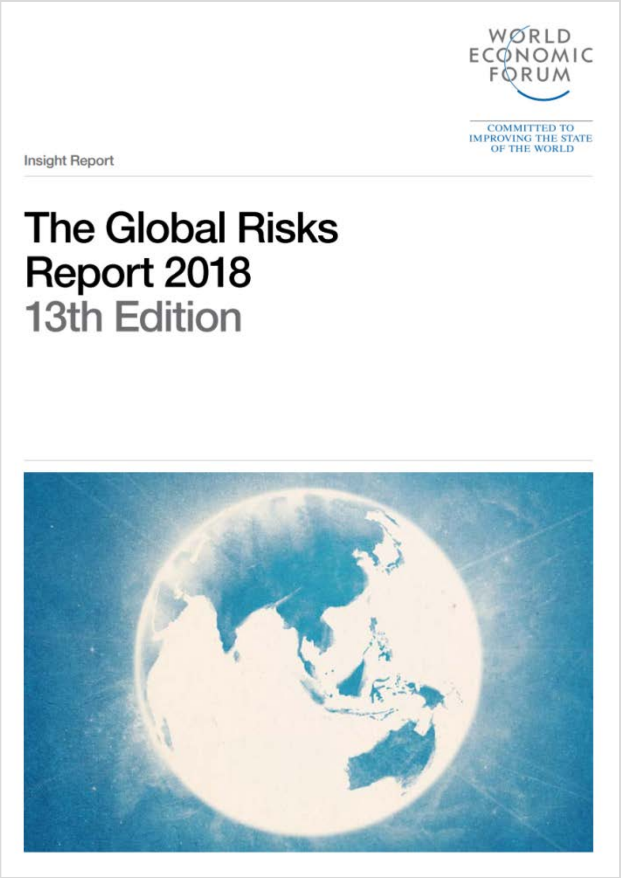


	NPP domains supported by computer systems					
	Physical Protection	Business	Operational	Safety	Emergency Response	Safeguards
	e.g. Access control system	e.g. Logistic system, Work permit system	e.g. Feedwater control system	e.g Reactor protection system	e.g Alarm system, Fire suppression system	e.g Video surveillance, NMAC
Assumed attacks targeted against domain	less	high	medium	less	less	less
Regulation on computer security	major improvements necessary	n/a	n/a	major improvements necessary	major improvements necessary	n/a
Standards/Guides on computer security	in progress	available	available	in progress	in progress	not available
Quality assurance program on computer security	part of regulation	standard level, improvements possible	not in regulation, improvements necess.	part of regulation	part of regulation	available
Qualification and training on computer security	insufficient	standard level, improvements possible	major improvements necessary	insufficient	insufficient	improvements possible
Education on computer security	major improvements necessary	partly available, improvements possible	partly available, improvements possible	partly available, improvements possible	major improvements necessary	major improvements necessary
Computer security operation and maintenance practices	insufficient	partly available, improvements possible	major improvements necessary	insufficient	insufficient	good
Computer intrusion detection	insufficient	major improvements necessary	major improvements necessary	insufficient	insufficient	major improvements necessary
Computer security incident response capability	insufficient	partly available, improvements possible	major improvements necessary	insufficient	insufficient	improvements possible
Computer security situational awareness and exercises	insufficient	partly available, improvements possible	major improvements necessary	insufficient	insufficient	insufficient
Computer security assessments and improvement	major improvements necessary	partly done, improvements possible	partly done, improvements possible	partly done, improvements possible	major improvements necessary	done

Source: G.Gluschke, ISS, April 2015

Is Cyber An Evolving And Emerging Threat?


Rising chronic diseases
Changing climate
Increasing national sentiment
Changing landscape of international governance
Biodiversity loss and ecosystem collapse
Degrading environment
Man-made environmental disasters
Natural disasters
Food crises
Extreme weather events
Spread of infectious diseases
Energy price shock
Failure of climate-change mitigation and adaptation
Water crises
Shifting power
Large-scale involuntary migration
Interstate conflict
Failure of urban planning
Weapons of mass destruction
Failure of regional or global governance
State collapse or crisis
Rising urbanization
Profound social instability
Failure of national governance
Failure of critical infrastructure
Terrorist attacks
Unmanageable inflation
Unemployment or underemployment
Adverse consequences of technological advances
Increasing polarization of societies
Critical information infrastructure breakdown
Cyberattacks
Deflation
Illicit trade
Fiscal crises
Growing middle class in emerging economies
Data fraud or theft
Asset bubbles in a major economy
Failure of financial mechanism or institution
Rising income and wealth disparity
Rising geographic mobility
Ageing population
Rising cyber dependency



WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

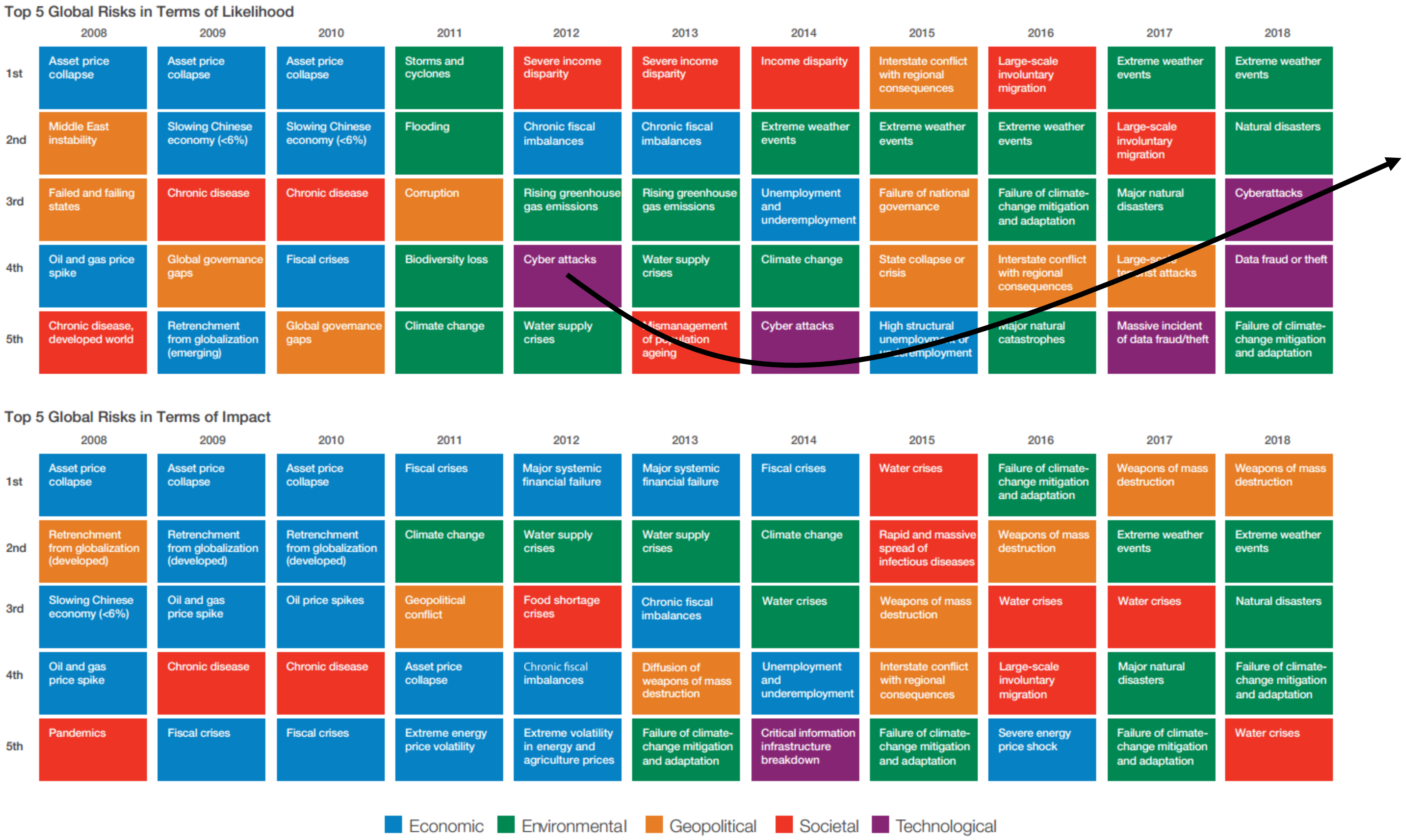
Insight Report

The Global Risks Report 2018
13th Edition

- ◆ Cyberattacks
- ◆ Data fraud or theft
- ◆ Adverse consequences of technological advances
- ◆ Critical information infrastructure breakdown

Source: World Economic Forum, The Global Risks Report 2018, 13th Edition

Is Cyber An Evolving And Emerging Threat?



Top 5 Global Risks in Terms of Likelihood

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
1st	🟦 Asset price collapse	🟦 Asset price collapse	🟦 Asset price collapse	🟩 Storms and cyclones	🟥 Severe income disparity	🟥 Severe income disparity	🟥 Income disparity	🟧 Interstate conflict with regional consequences	🟥 Large-scale involuntary migration	🟩 Extreme weather events	🟩 Extreme weather events
2nd	🟧 Middle East instability	🟦 Slowing Chinese economy (<6%)	🟦 Slowing Chinese economy (<6%)	🟩 Flooding	🟦 Chronic fiscal imbalances	🟦 Chronic fiscal imbalances	🟩 Extreme weather events	🟩 Extreme weather events	🟩 Extreme weather events	🟥 Large-scale involuntary migration	🟩 Natural disasters
3rd	🟧 Failed and failing states	🟥 Chronic disease	🟥 Chronic disease	🟧 Corruption	🟩 Rising greenhouse gas emissions	🟩 Rising greenhouse gas emissions	🟦 Unemployment and underemployment	🟧 Failure of national governance	🟩 Failure of climate-change mitigation and adaptation	🟩 Major natural disasters	🟪 Cyberattacks
4th	🟦 Oil and gas price spike	🟧 Global governance gaps	🟦 Fiscal crises	🟩 Biodiversity loss	🟪 Cyber attacks	🟩 Water supply crises	🟩 Climate change	🟧 State collapse or crisis	🟧 Interstate conflict with regional consequences	🟧 Large-scale terrorist attacks	🟪 Data fraud or theft
5th	🟥 Chronic disease, developed world	🟦 Retrenchment from globalization (emerging)	🟧 Global governance gaps	🟩 Climate change	🟩 Water supply crises	🟥 Mismanagement of population ageing	🟪 Cyber attacks	🟦 High structural unemployment or underemployment	🟩 Major natural catastrophes	🟪 Massive incident of data fraud/theft	🟩 Failure of climate-change mitigation and adaptation

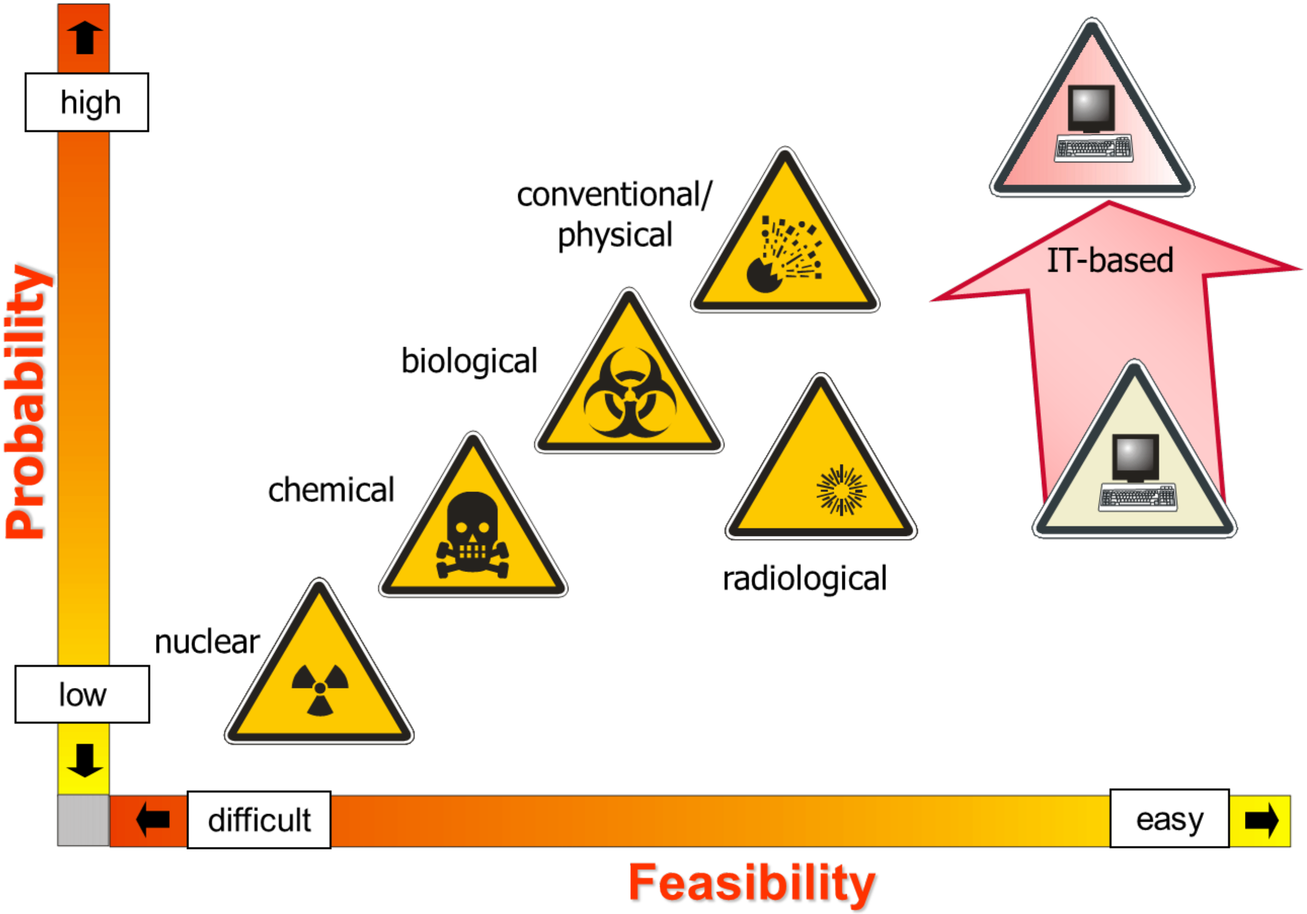
Top 5 Global Risks in Terms of Impact

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
1st	🟦 Asset price collapse	🟦 Asset price collapse	🟦 Asset price collapse	🟦 Fiscal crises	🟦 Major systemic financial failure	🟦 Major systemic financial failure	🟦 Fiscal crises	🟥 Water crises	🟩 Failure of climate-change mitigation and adaptation	🟧 Weapons of mass destruction	🟧 Weapons of mass destruction
2nd	🟧 Retrenchment from globalization (developed)	🟦 Retrenchment from globalization (developed)	🟦 Retrenchment from globalization (developed)	🟩 Climate change	🟩 Water supply crises	🟩 Water supply crises	🟩 Climate change	🟥 Rapid and massive spread of infectious diseases	🟧 Weapons of mass destruction	🟩 Extreme weather events	🟩 Extreme weather events
3rd	🟦 Slowing Chinese economy (<6%)	🟦 Oil and gas price spike	🟦 Oil price spikes	🟧 Geopolitical conflict	🟥 Food shortage crises	🟦 Chronic fiscal imbalances	🟩 Water crises	🟧 Weapons of mass destruction	🟥 Water crises	🟥 Water crises	🟩 Natural disasters
4th	🟦 Oil and gas price spike	🟥 Chronic disease	🟥 Chronic disease	🟦 Asset price collapse	🟦 Chronic fiscal imbalances	🟧 Diffusion of weapons of mass destruction	🟦 Unemployment and underemployment	🟧 Interstate conflict with regional consequences	🟥 Large-scale involuntary migration	🟩 Major natural disasters	🟩 Failure of climate-change mitigation and adaptation
5th	🟥 Pandemics	🟦 Fiscal crises	🟦 Fiscal crises	🟦 Extreme energy price volatility	🟦 Extreme volatility in energy and agriculture prices	🟩 Failure of climate-change mitigation and adaptation	🟪 Critical information infrastructure breakdown	🟩 Failure of climate-change mitigation and adaptation	🟦 Severe energy price shock	🟩 Failure of climate-change mitigation and adaptation	🟥 Water crises

🟦 Economic 🟩 Environmental 🟧 Geopolitical 🟥 Societal 🟪 Technological

Source: World Economic Forum, The Global Risks Report 2018, 13th Edition

Is Cyber An Evolving And Emerging Threat?



What Picture Gives Us A Good Understanding In Terms Of Cyber Defense?

Picture: https://www.carsharing-news.de/carsharing-bonn/

What Picture Gives Us A Good Understanding In Terms Of Cyber Defense?

- In term of complexity we can visualize the problem of cyber defence by using a known structure – a „Cyber Town“
  - thousends of buildings which are our networked components with streets connecting all buildings
  - historically grown structures
  - each building and street has its own characteristics and has to be protected differently
  - there is no central assessment of all parameters you need to protect such an environment
  - beside buildings we like to protect cars which represents communication equipment on the data transport layer and people which are the information assets in our model
- How many threats with its different attack vectors exist? How hard is it to protect such an environment? How much preparation do you need? How many changes will take place over time?

How do You Know If Your Communication Equipment (Firewall) Is Good Enough?

Picture: G. Gluschke

And What Are You Still Able To See Under Attack?

Picture: G. Gluschke

How To Control Your „Cyber Town“ Against Attacks?
What Is Your Response To A Modern Cyber Bomb?

Picture: https://de.sputniknews.com/politik/20170720316679706-russland-usa-syrien-putins-sieg-medien/

Is A Full-scope Cyber Threat Assessment Possible?

- Example: Focusing on a facility, not on IoT
- Not considering different threat actors with their motivation, willingness, funding etc., only focusing on attack vectors
- Not considering data/information, scope only on IT/OT systems
- In a real IT/OT environment we will find
  - various vendors with their own technology
  - various hardware plattforms
  - various firmware versions
  - various I/O interfaces and connectivity
  - various operating systems
  - various human-machine-interfaces
  - various applications
- Considering this IT/OT parameters, hundreds of attack vectors in order to manipulate or destroy exist

Is A Full-scope Cyber Threat Assessment Possible?

- Around 25.000 digital components in a Gen II PWR
  - Assumed, one digital component relates to one attack vector
  - Cyber threats to assess with only ONE! attack vector: 25.000 => Likely possible
- Various IT/OT-parameters in conjunction with security objectives (e.g. CIA) build attack vectors which have to be assessed
  - Considering TEN attack vectors: $10^{25.000}$ => Far too much
- Probably grouping of components might help: Realistic grouping results in 800 groups of IT/OT components
  - Considering TEN attack vectors: 10^{800} => Still too much

A full-scope assessment of cyber threats (attack vectors) cannot be conducted easily. We can try to assess the impact of a cyber threat and the effectiveness of protective measures against cyber threats.

Are The Attributes And Characteristics From NSS10 (DBT) Applicable For Cyber?

- Motivation: political, financial, ideological, personal;
- Willingness to put one’s own life at risk;
- Intentions: sabotage of a facility, theft, causing public panic and social disruption, instigating political instability, causing mass injuries and casualties;
- Group size: attack force, coordination personnel, support personnel;
- Weapons: types, numbers, availability;
- Explosives: type, quantity, availability, triggering sophistication, acquired or improvised;
- Tools: mechanical, thermal, manual, power, electronic, electromagnetic, communications equipment;
- Modes of transportation: public, private, land, sea, air, type, number, availability;

- Technical skills: engineering, use of explosives, chemicals, paramilitary experience, communications skills;
- ‘Cyber’ skills: skills in using computer and automated control systems in direct support of physical attac
  gathering, for c
  money gatherin
- Knowledge: targ
  procedures, security measures, safety measures and radiation protection procedures, operations, potential use of nuclear or other
- Funding: source
- Insider threat is
  active involvement, violent or non-violent engagement, number of insider adversaries;
- Support structu
  local sympathiz
  logistical suppo
- Tactics: use of s

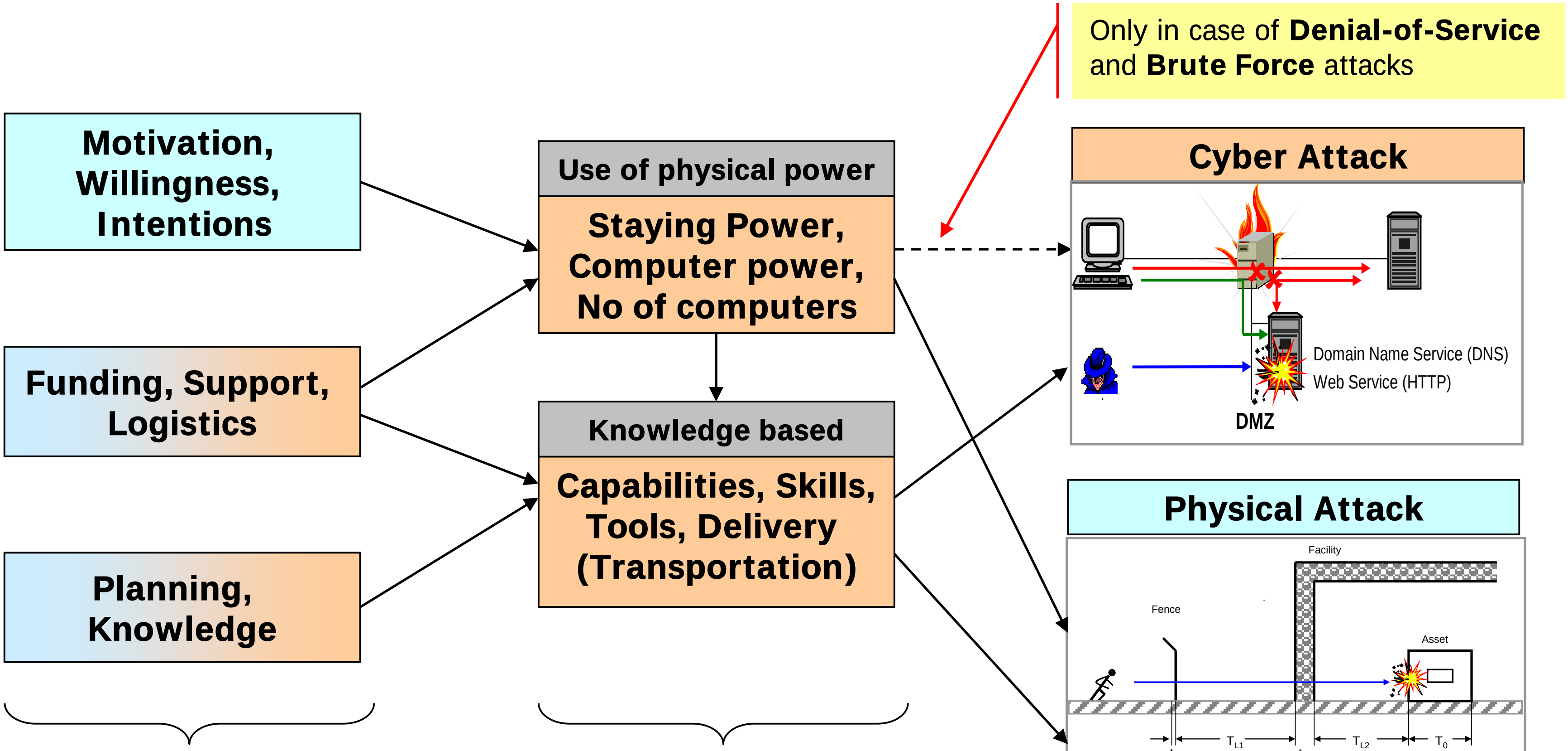
'Weapons' can be understood as 'cyber-weapons' but no general definition therefore exists

'Explosives' can not be easily mapped to the cyber world;

'Modes of transportation' in a physical meaning might be applied to the delivery of maleware, e.g. by devices such as USB sticks

green = apply to cyber in a similar meaning
orange = apply to cyber in another meaning
red = do not apply to cyber

Are The Attributes And Characteristics From NSS10 (DBT) Applicable For Cyber?



Only in case of **Denial-of-Service** and **Brute Force** attacks

Motivation, Willingness, Intentions

Funding, Support, Logistics

Planning, Knowledge

Use of physical power

Staying Power, Computer power, No of computers

Knowledge based

Capabilities, Skills, Tools, Delivery (Transportation)

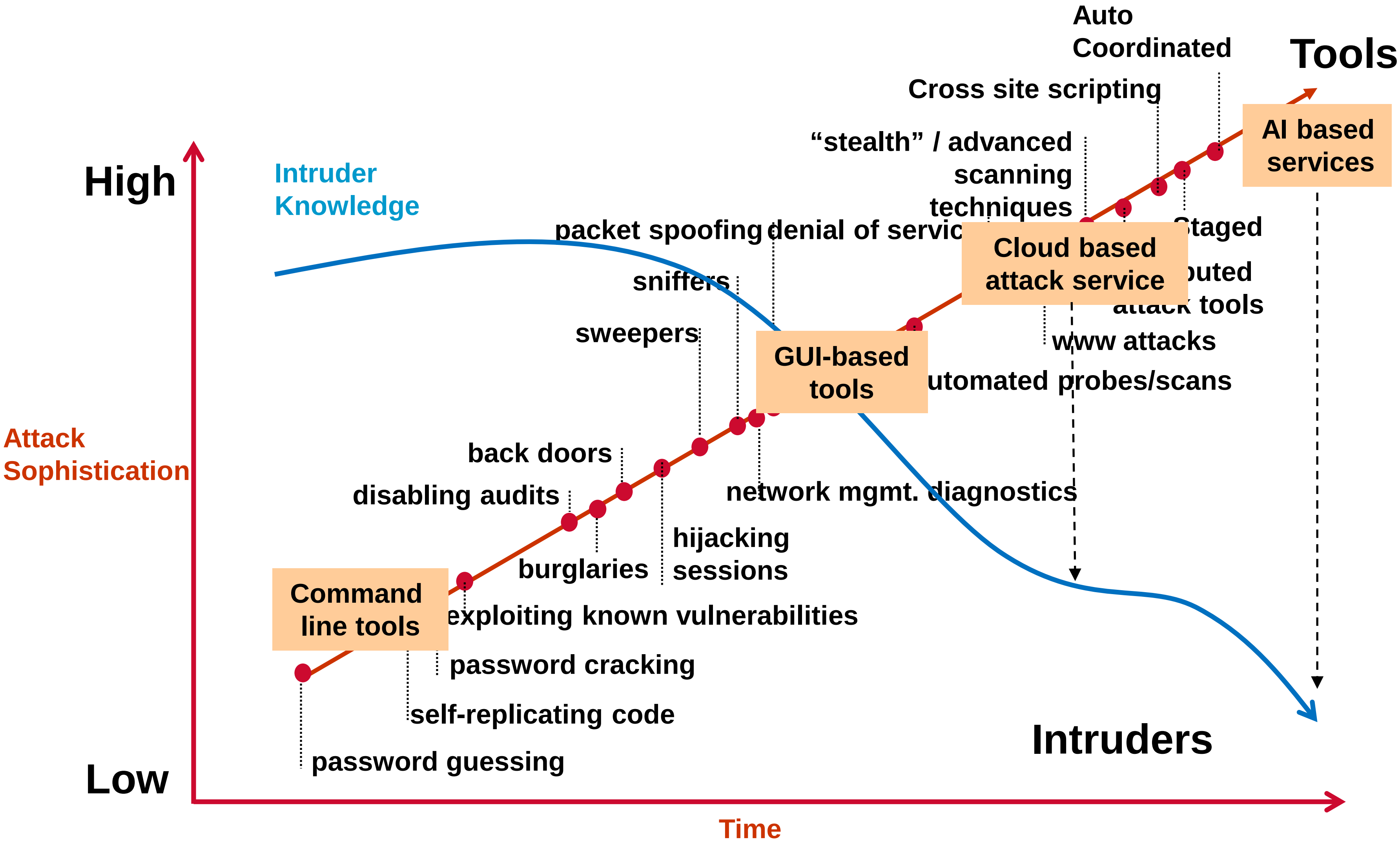
Cyber Attack

Physical Attack

Indirect impact on attacked asset

Direct impact on attacked asset

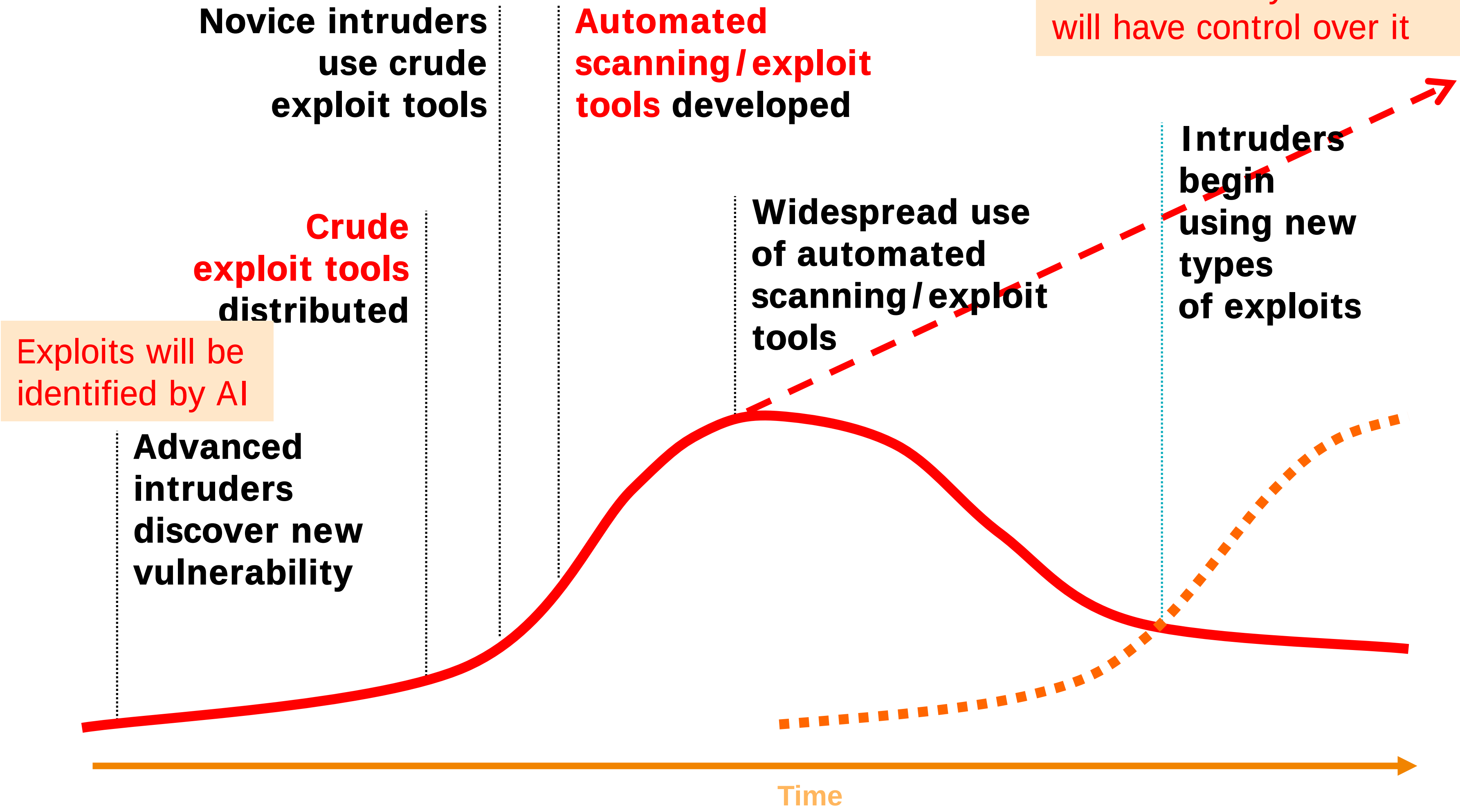
How Is Attack Sophistication vs. Intruder Technical Knowledge Evolving?



Source: Carnegie Mellon University

What Will Change From The Classic Vulnerability Exploit Cycle?

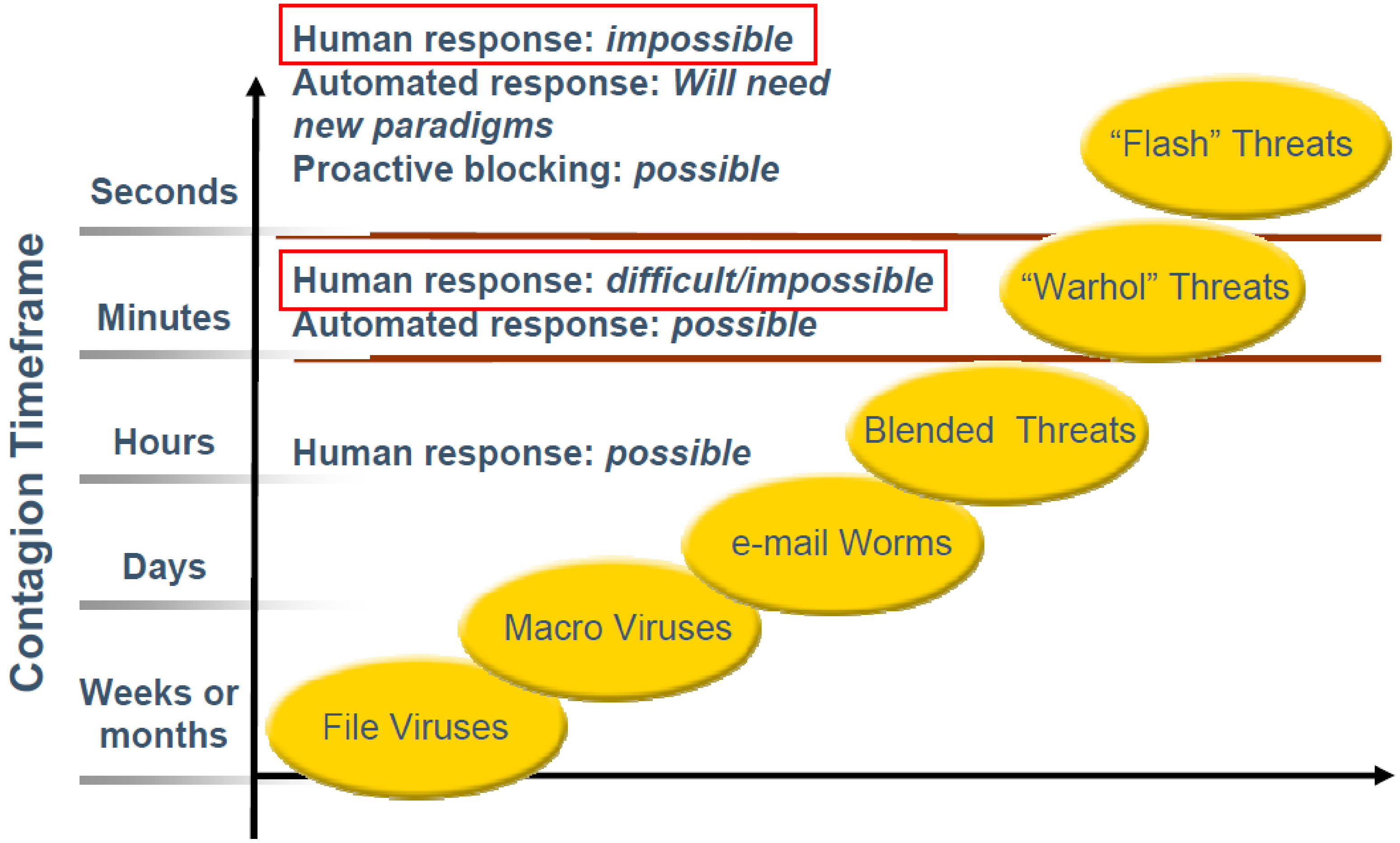
Exploits will be used as part of a larger game and autonomous systems will have control over it



Exploits will be identified by AI

Source: Carnegie Mellon University

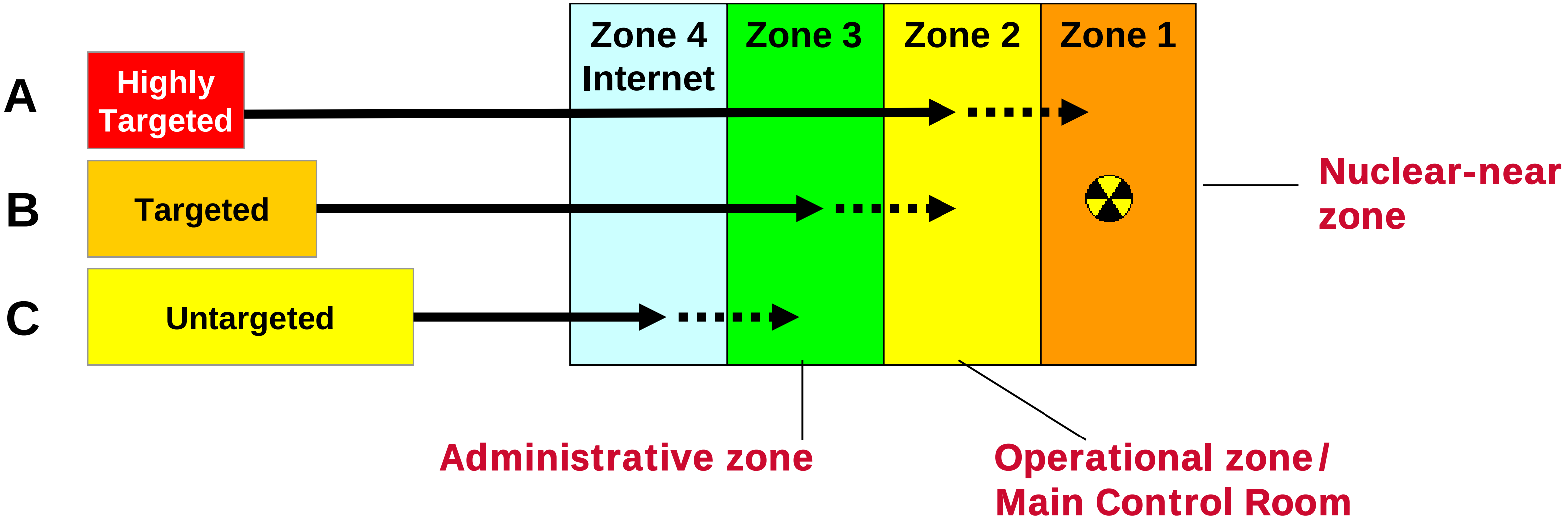
What Is About The Response Time To Cyber Threats?



Human response: *impossible*
Automated response: *Will need new paradigms*
Proactive blocking: *possible*
Seconds
Minutes
Human response: *difficult/impossible*
Automated response: *possible*
Hours
Human response: *possible*
Days
Weeks or months
Contagion Timeframe
"Flash" Threats
"Warhol" Threats
Blended Threats
e-mail Worms
Macro Viruses
File Viruses

Source: Carnegie Mellon University

Can We Keep Cyber Attacks Under Control?



A Highly targeted: Targeted against a particular component / system[1]

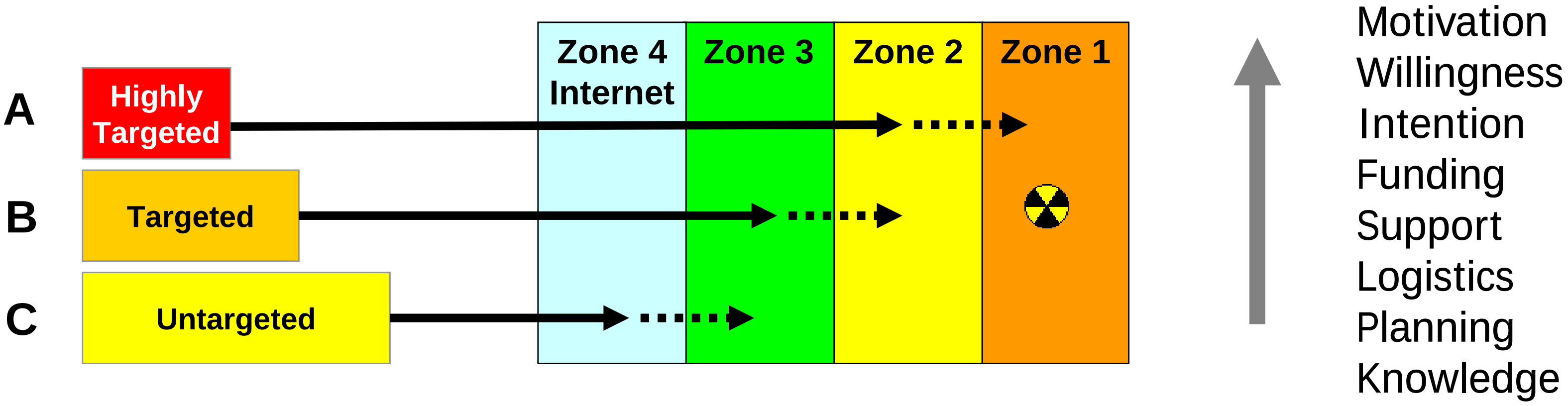
B Targeted: Targeted against a particular organization / facility[2]

C Untargeted: Not targeted against particular organization / facility (Random target / Target of opportunity)

[1] e.g. The Stuxnet incident: see http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[2] e.g. The Monju incident: see https://www.contextis.com//resources/blog/context-threat-intelligence-monju-incident/

Can We Keep Cyber Attacks Under Control?



A Highly targeted: Military-style adversary (Threat is invisible / not understood yet)
B Targeted: Traditional adversary groups (Threat is partly visible / basically understood)
C Untargeted: Everyone else (Threat is well understood)

A Highly targeted*: no prevention, advanced detection and response
B Targeted: extended prevention, advanced detection and response**
C Untargeted: standard prevention, detection and response

***State-of-the-art controls are ineffective (by definition), individual controls might help**
****State-of-the-art controls are effective but not sufficient, additional individual controls necessary**

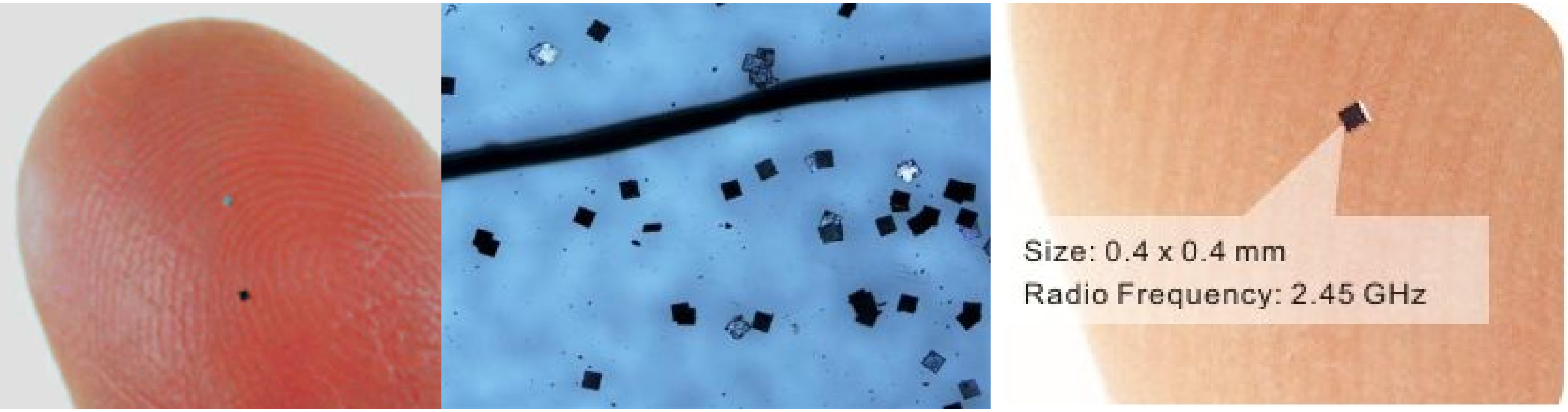
What Is The Current Situation In Terms Of Cyber Threats?

- Nuclear facilities are complex system, more and more digitalized parts, in particular in ICS, increased internet connectivity
- Cyber as a new domain of military actions, Industrial Control Systems (ICS/I&C) as new targets
- Cyber attacks invisible, rapidly changing, very professional
- Effective tools for cyber prevention and detection are missing
- Individual attacks, addressing human, IT/OT and business processes, categorization and attribution difficult
- Sufficient cyber security/defense knowledge often not available at the facility (e.g. for incident response)
- Responsibilities for different levels of cyber defense unclear in most nation states, unclear definitions, insufficient understanding of circumstances
- Methodologies for threat analysis and prediction lacking

What Are Examples For Future Cyber Threats?

- End of asymmetric encryption
  - Researchers need only five quantum bits for prime factorization - the end of RSA encryption is approaching
- Proliferation of AI
  - Artifcial intelligence “weeds” proliferate, choking off the performance of the internet, AI based software bots living in your networks
- War without rules
  - State-on-state cyberattacks escalate unpredictably owing to a lack of agreed protocols, hybrid warfare
  - Use of drones to attack networks remotly
  - AI fights against AI
- Organisations identify vulnerabilties and produce cyber attacks by listening to data streams and by analysing it, autonomous systems use it to attack
- New „cyber cold war“ on the border of the BRIC internet

Is This A Cyber Threat?



Size: 0.4 x 0.4 mm

Radio Frequency: 2.45 GHz

Source: PSD

Technische Hochschule
Brandenburg
University of
Applied Sciences
Institute for Security
and Safety

Evolving and Emerging Cyber Threats

Thank you for your attention!

g.gluschke@uniss.org
www.uniss.org