WiCR
Women must have a place at the table

Critical infrastructure, interconnected risks, and resiliency.

Why wo(men) should care?

WiCR
Women must have a place at the table

A little bit about me ☺

Me as a kid!! ;)

Life happens and its tough! :)

- I identify as South-Asian woman from Mumbai, India. I started off in my computer career as a data entry operator for a brief period right out of my vocational college where I got a diploma in Computer Science and Engineering in 1995.
- Later working as lab programmer, software engineer, analyst, subject matter expert, consultant, etc., slowly progressed through various roles within IT and IS whilst pursuing a Masters in Computer Applications back then.
- I wanted to become an Aeronautical Engineer, study astrophysics and work for NASA; well but that never happened, as evident! ☺ I became an IT/IS expert instead and consulted on security risks for applications and systems and I really enjoyed my job and work as a cybersecurity subject matter expert – am now just a different type of engineer!!
- I had to drop out of my master's program due to socioeconomic conditions that made it impossible to work and study or bear the cost of my education anymore, and the educational loan system was not accessible to me at that time.

Me in 2011 ;)

Me in 2020 :)

- Many years later in 2016, I went back to one of my dream schools– **Harvard University**, and through their continuing education department as an experienced adult who wanted to work on her life’s purpose, decided to get a degree in Economics with Government and International Security specialisation.
- Here I worked on all the ideas that had been brewing in my head for all these years!!
- Towards the end of my study in 2020, I founded, “**Women in Crisis Response**” on the core principles of UNSCR 1325 and Human Security, to fulfill my purpose of helping women and girls achieve safety and security in lie by helping them break the barriers that hold them back from development, both in career and in personal lives, so that other girls who dream of becoming who they want to become have the support to help them fulfill their potential.

WiCR
Women must have a place at the table

Presentation layout

- Critical Infrastructure, Industry 4.0, Cybersecurity – Understanding the terms and interrelationships
- Understanding interconnected threats and vulnerabilities
- Cognitive and other socio-structural limitations
- Building resilience through preparedness and capacity planning
- Understanding Gaps
- Addressing barriers to entry and thrive in the industry – Gender perspective
- Appendix

What is Critical Infrastructure?

- Critical Infrastructure are essential public services such as hospitals, banking, schools, electricity grids, water treatment plants etc.,

Why talk about this?

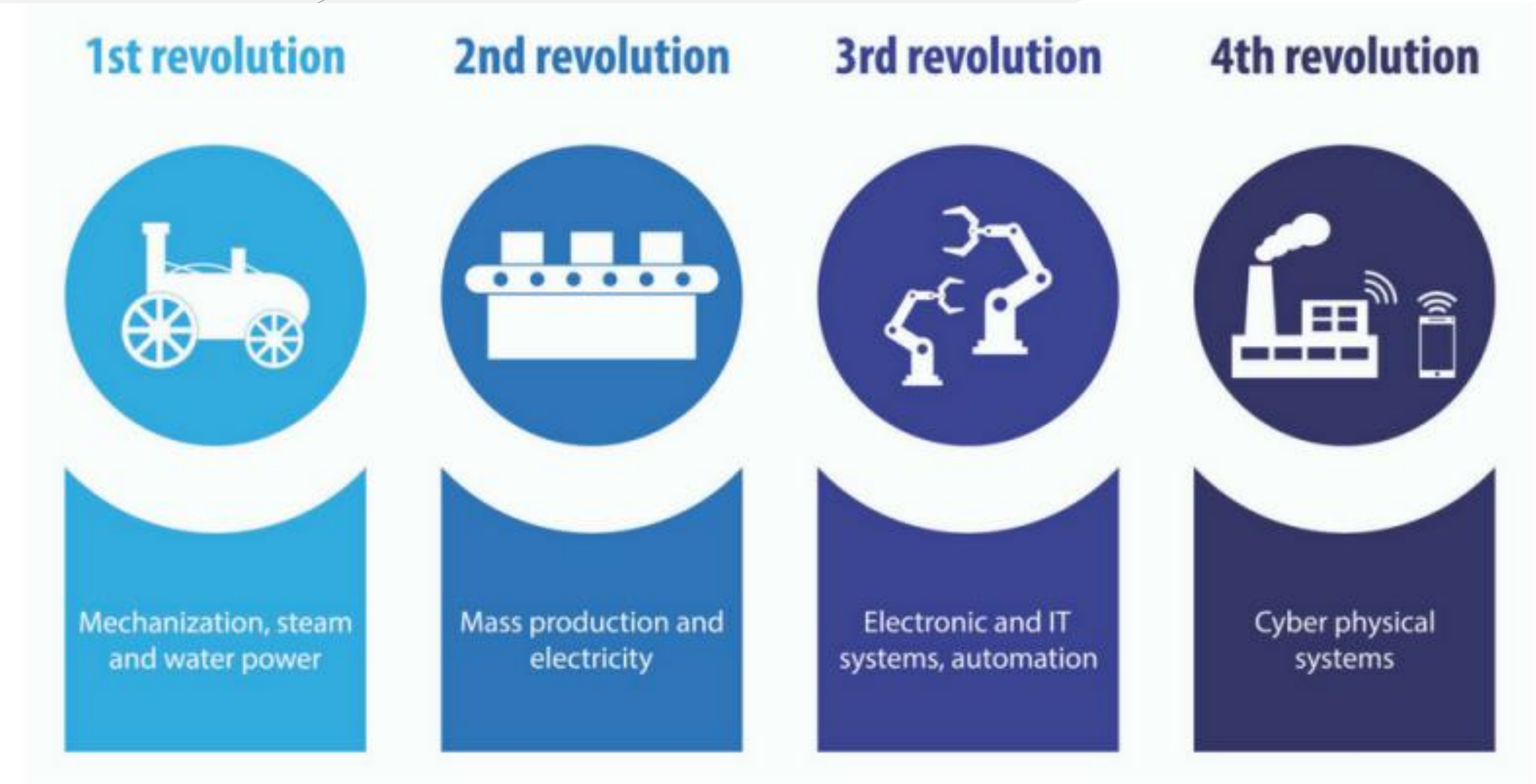
- Traditionally, these public and civil services have existed in our physical world for hundreds of years but are now increasingly being interconnected via the internet and automated. This forms the core of what we now call Industry 4.0

Here’s a very good definition from the UK Centre for Protection of National Infrastructure

- National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends.
- It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example).

https://www.cpni.gov.uk/critical-national-infrastructure-0

Industry 4.0


1st revolution
2nd revolution
3rd revolution
4th revolution
Mechanization, steam and water power
Mass production and electricity
Electronic and IT systems, automation
Cyber physical systems

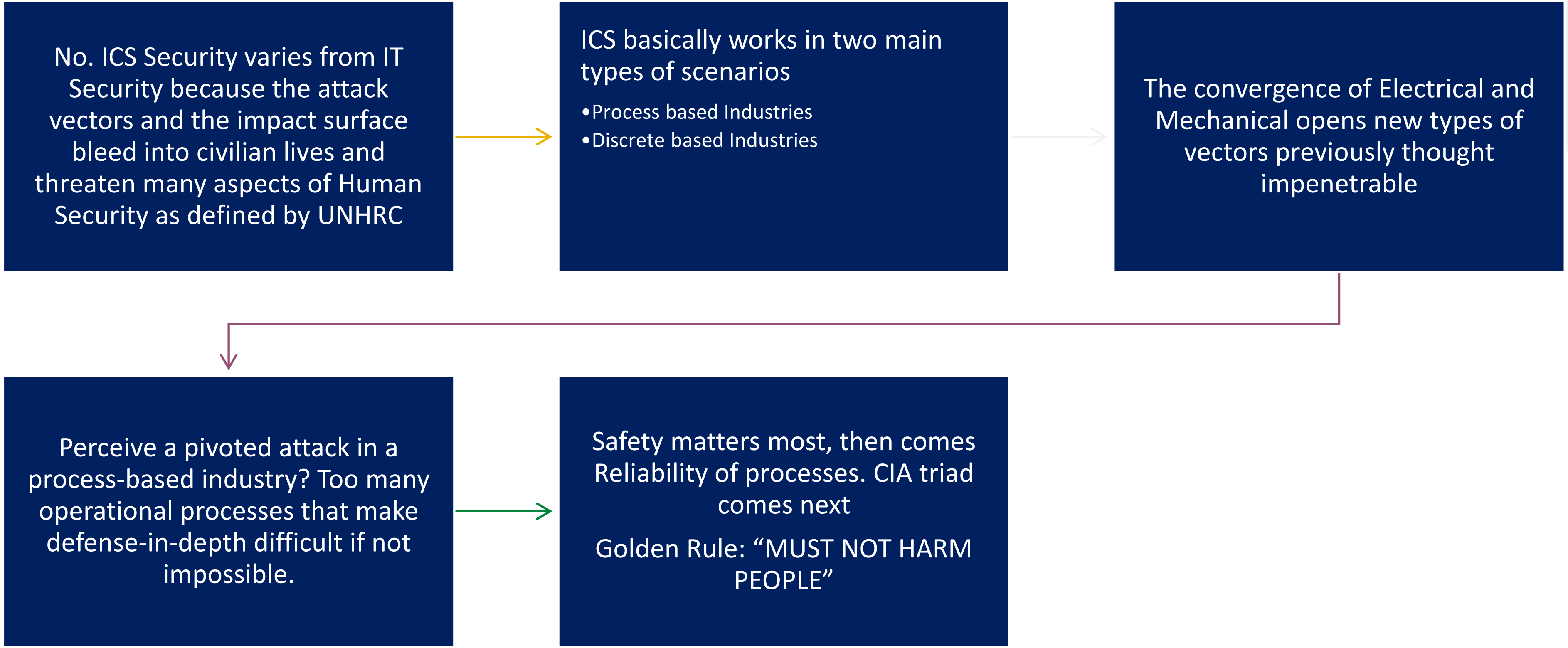
https://pattiengineering.com/blog/faqs-on-iiot/

Industrial Control Systems (ICS)

- Industrial control systems are a set of components, devices, and systems that together control, administer, and manage the critical infrastructure. A typical ICS consists of the following systems:
  - Process Control System (PCS)
  - Distributed Control Systems (DCS)
  - Programmable Logic Controllers (PLC)
  - Supervisory Control and Data Acquisition (SCADA)
  - Safety Instrumented Systems (SIS)
  - Human Machine Interface (HMI)
  - Remote Terminal Unit (RTU)

https://www.msec.be/verboten/seminaries/ICS_archs_and_sec_essentials/ICS_Overview.pdf

ICS Security, is it not the same as IT Security?



No. ICS Security varies from IT Security because the attack vectors and the impact surface bleed into civilian lives and threaten many aspects of Human Security as defined by UNHRC

ICS basically works in two main types of scenarios

- Process based Industries
- Discrete based Industries

The convergence of Electrical and Mechanical opens new types of vectors previously thought impenetrable

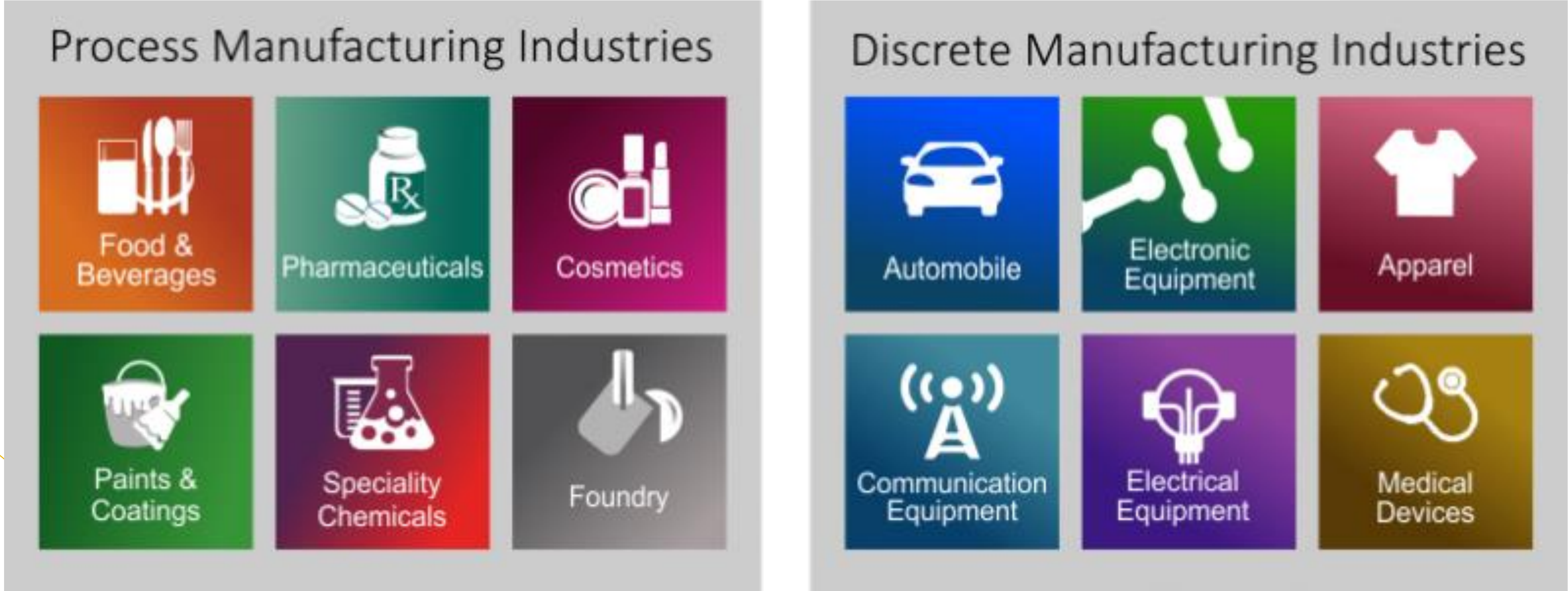
Perceive a pivoted attack in a process-based industry? Too many operational processes that make defense-in-depth difficult if not impossible.

Safety matters most, then comes Reliability of processes. CIA triad comes next

Golden Rule: “MUST NOT HARM PEOPLE”

NIST Guide to [Industrial Control Systems (ICS) Security]

Process vs Discrete based industry



Process Manufacturing Industries

- Food & Beverages
- Pharmaceuticals
- Cosmetics
- Paints & Coatings
- Speciality Chemicals
- Foundry

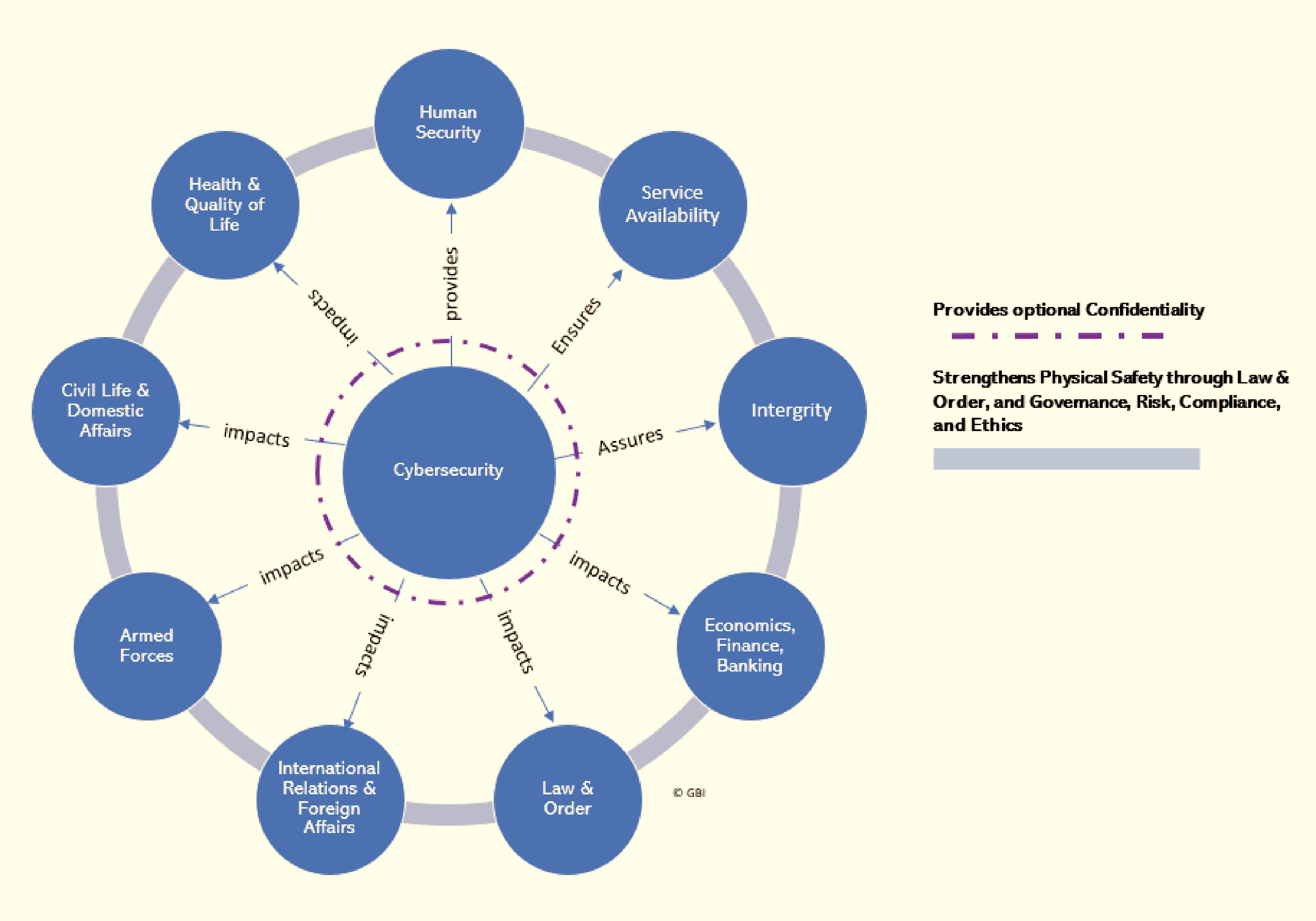
Discrete Manufacturing Industries

- Automobile
- Electronic Equipment
- Apparel
- Communication Equipment
- Electrical Equipment
- Medical Devices

https://www.batchmaster.co.in/blog/difference-between-discrete-and-process-manufacturing/

WiCR
Women must have a place at the table

Cybersecurity permeates many aspects of our lives



Human Security
Health & Quality of Life
Service Availability
Civil Life & Domestic Affairs
Intergrity
Cybersecurity
Armed Forces
Economics, Finance, Banking
International Relations & Foreign Affairs
Law & Order
provides
impacts
Ensures
impacts
Assures
impacts
impacts
impacts
impacts
Provides optional Confidentiality
Strengthens Physical Safety through Law & Order, and Governance, Risk, Compliance, and Ethics
© GBI

And why should we as civilians care?

- Internet of Things blurs the line between Electrical and Mechanical
- What were secure through obscurity are now deemed unsecure for the very same reasons
- Engineering, Operational, Architecture, and Design professionals can no more detach themselves from the matters of security
- As they embark on designing infrastructure for cities and industrial systems, thinking about safety, security, and privacy becomes essential

And we depend on these services on a daily basis

So what?

- And What are the risks of connecting these devices to the internet after all?

Internet of Things?

- IoT and IIoT – Do we really need our personal coffee maker, our toaster, our refrigerator, or our TV on the internet?

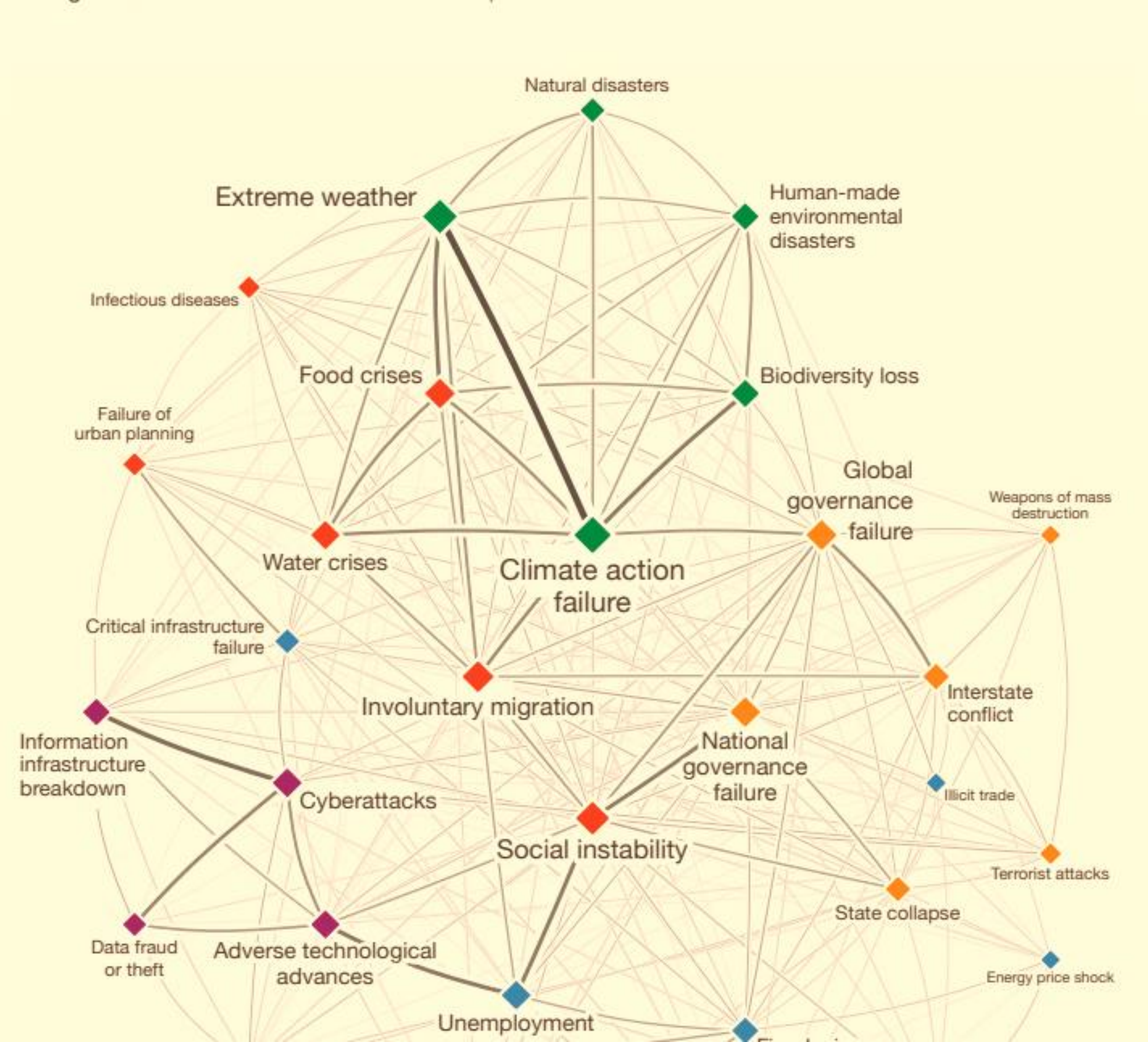
WiCR
Women must have a place at the table

Understanding Risks

Risk, Threat, Vulnerability, Impact, Likelihood

WiCR
Women must have a place at the table

Understanding interconnected risks



Source: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf p5

WiCR
Women must have a place at the table

Defense and military organisations like NATO have formally recognized Cyberspace* as a new frontier in defense, along with land, air and sea, meaning battles could henceforth be waged on computer networks

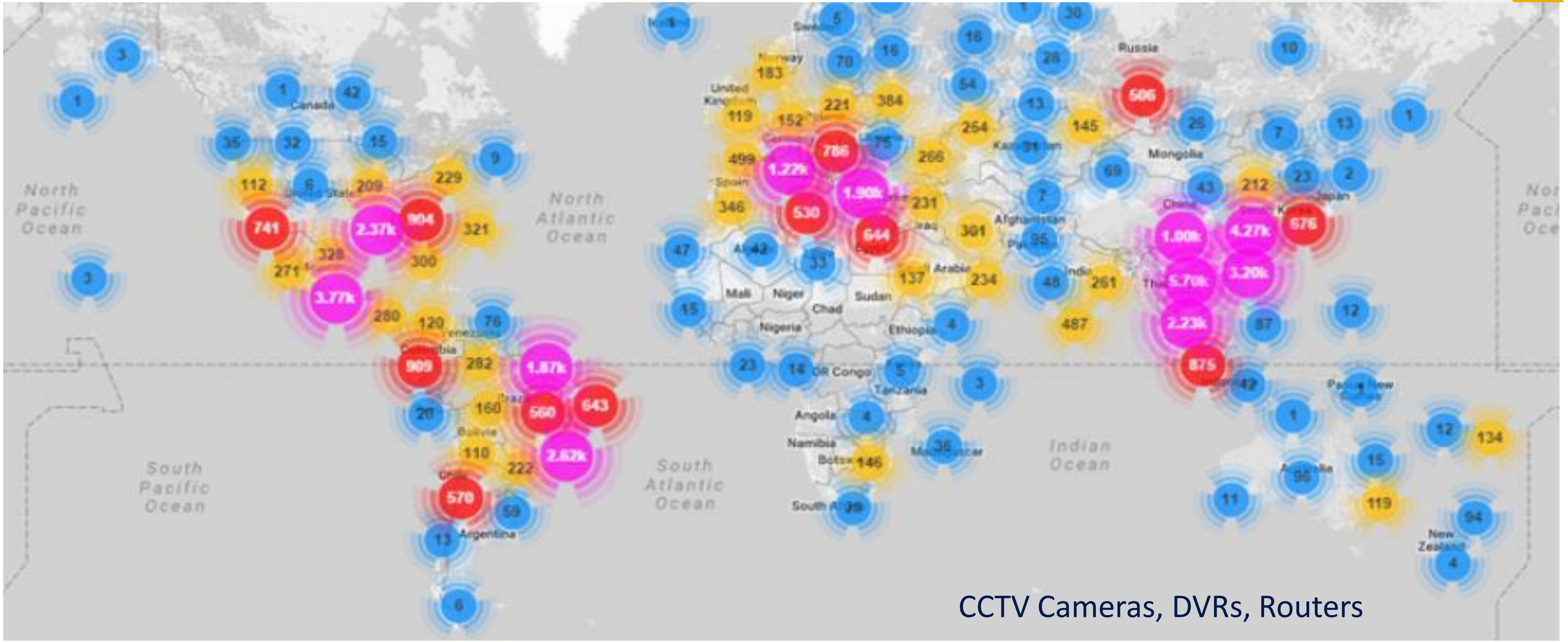
This means that the alliance could use cyber weapons to manage global threats to systems and infrastructure used by NATO allies (North America and European countries)

So what about other countries? Are they prepared?

Is the civilian world ready for the impact from new generation warfare?

* Source: https://www.nato.int/cps/en/natohq/topics_78170.htm

This Is Not A Map Of Coronavirus Infections – This Is Computer Virus! Mirai Botnet Infections Around The World In 2016

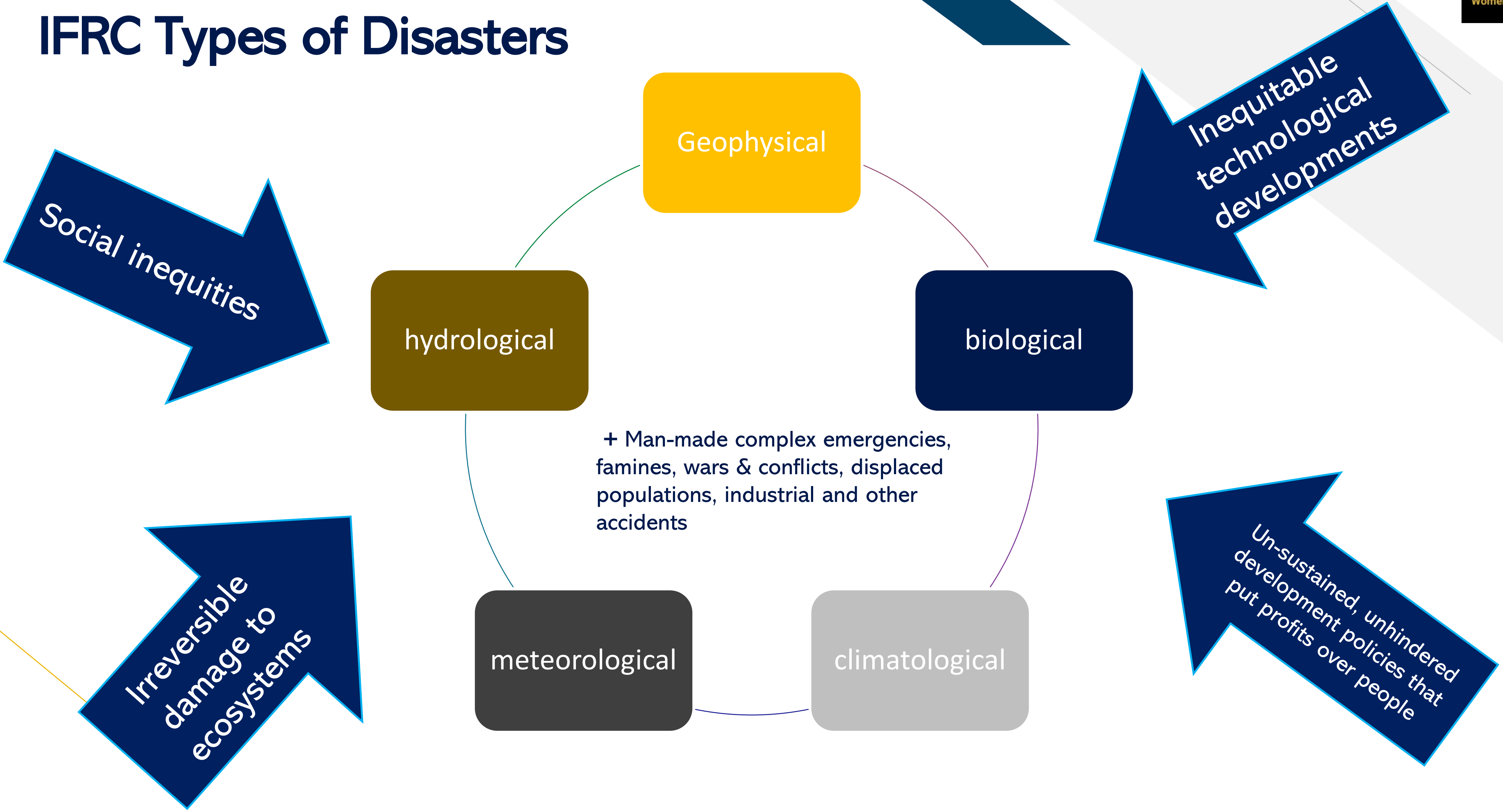


CCTV Cameras, DVRs, Routers

Source: https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/
https://www.vice.com/en_us/article/9a3zy8/heres-a-live-map-of-the-mirai-malware-infecting-the-world

WiCR
Women must have a place at the table

IFRC Types of Disasters


Geophysical
biological
climatological
meteorological
hydrological
Social inequities
Inequitable technological developments
Un-sustained, unhindered development policies that put profits over people
Irreversible damage to ecosystems

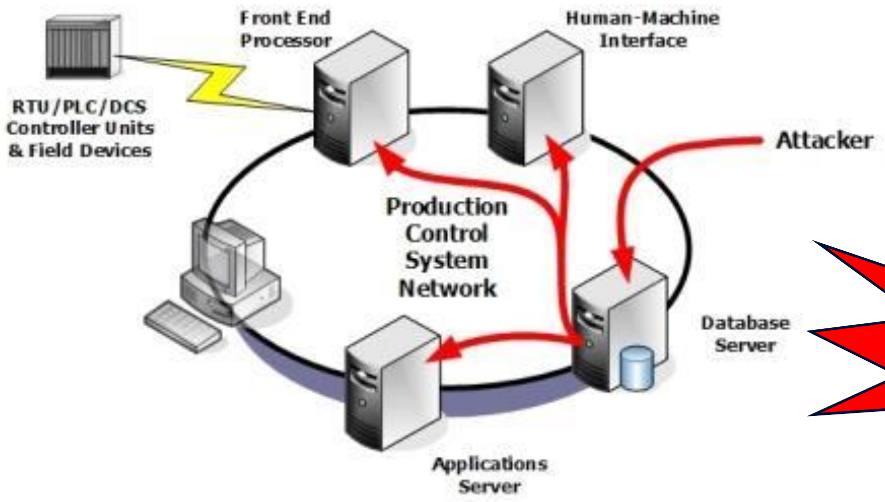
+ Man-made complex emergencies, famines, wars & conflicts, displaced populations, industrial and other accidents

Accelerate, increase frequency, complexity, and severity of the disasters

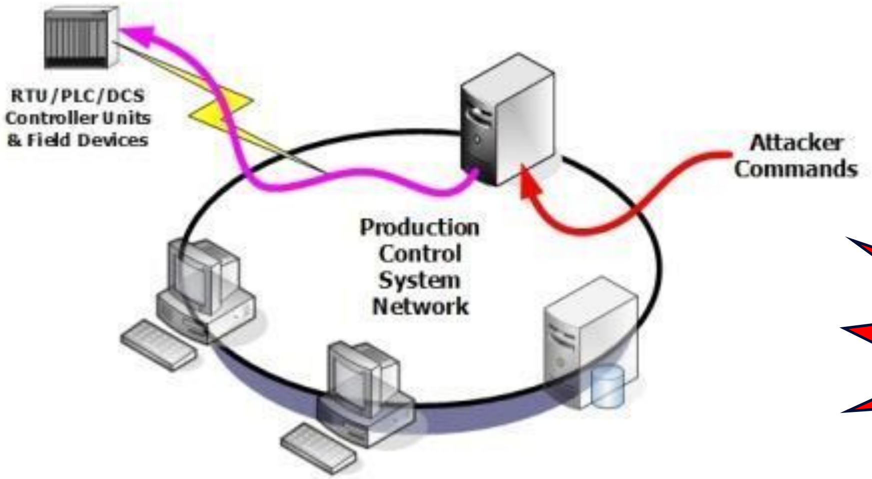
https://www.ifrc.org/en/what-we-do/disaster-management/about-disasters/definition-of-hazard/

Cyber Vulnerabilities

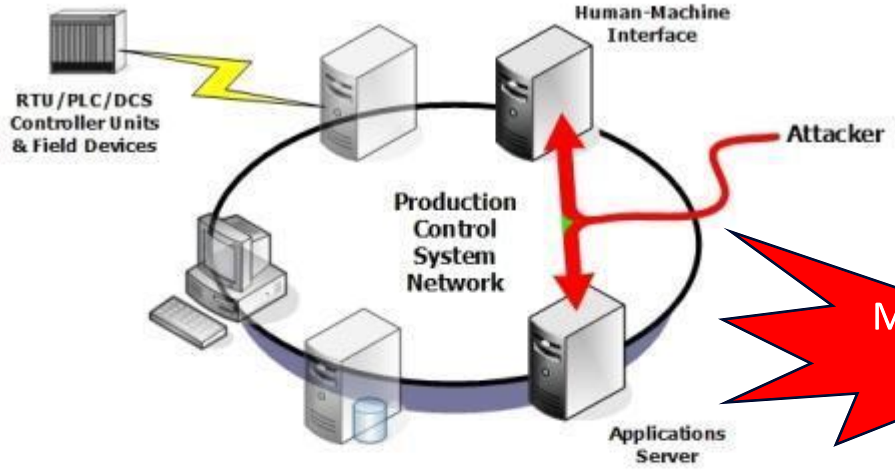
https://www.us-cert.gov/ics/content/overview-cyber-vulnerabilities



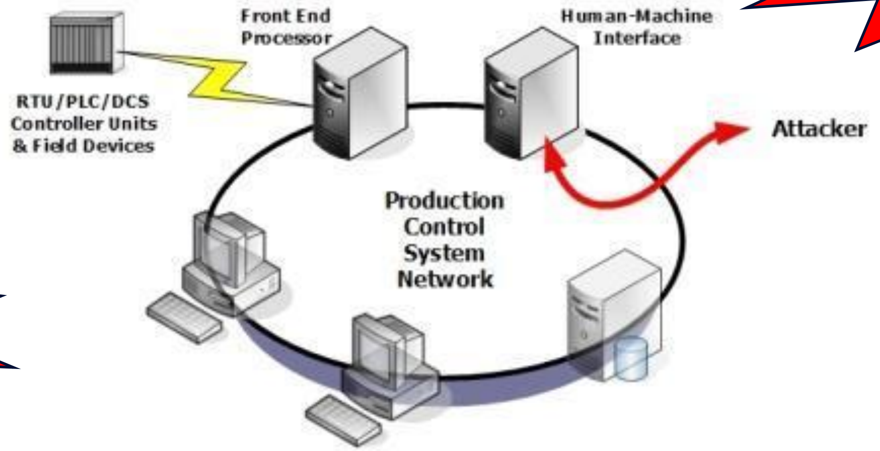
Changing the database


RTU/PLC/DCS Controller Units & Field Devices
Attacker Commands
Production Control System Network

Sending commands directly


Human-Machine Interface
RTU/PLC/DCS Controller Units & Field Devices
Attacker
Production Control System Network
Applications Server

Man-in-the-middle


Front End Processor
Human-Machine Interface
RTU/PLC/DCS Controller Units & Field Devices
Attacker
Production Control System Network

Exporting HMI Screen

Mobile Phones have their own problems!

Mobile Top 10 2016-Top 10

M1 - Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.
M2 - Insecure Data Storage	This new category is a combination of M2 + M4 from Mobile Top Ten 2014. This covers insecure data storage and unintended data leakage.
M3 - Insecure Communication	This covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.
M4 - Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: • Failing to identify the user at all when that should be required • Failure to maintain the user's identity when it is required • Weaknesses in session management
M5 - Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasn't done correctly.
M6 - Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.
M7 - Client Code Quality	This was the "Security Decisions Via Untrusted Inputs", one of our lesser-used categories. This would be the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.
M8 - Code Tampering	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.
M9 - Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.
M10 - Extraneous Functionality	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.

https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

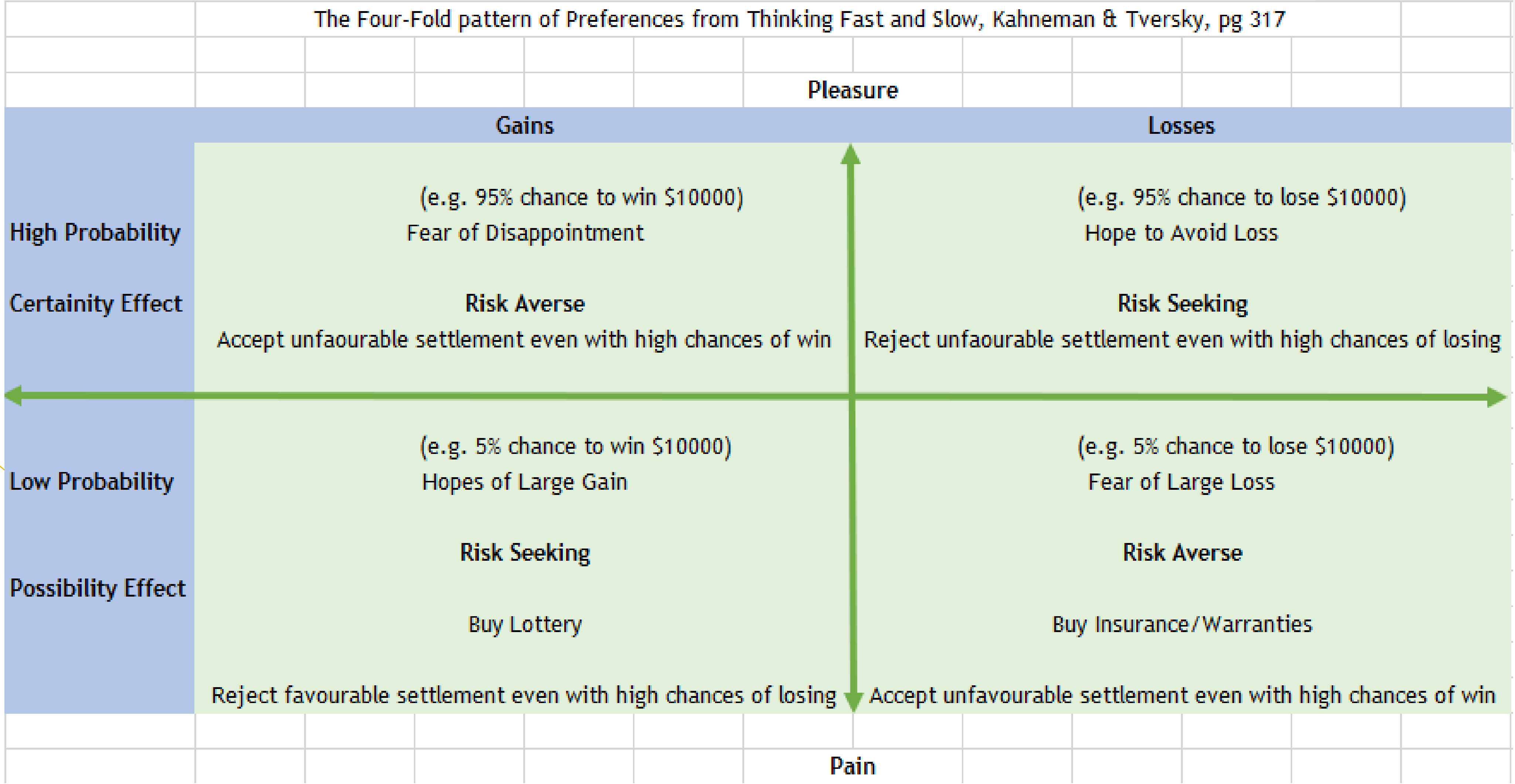
- Networking Protocols have limitations
- Back compatibility and forward compatibility are bigger issues
- Software maintenance brings additional complexity in highly interconnected systems especially if they are coupled with ICS systems

Fact: Humans have cognitive limitations

AI code can also have these bias and limitations built in as a result.

WiCR
Women must have a place at the table

Humans are fallible!



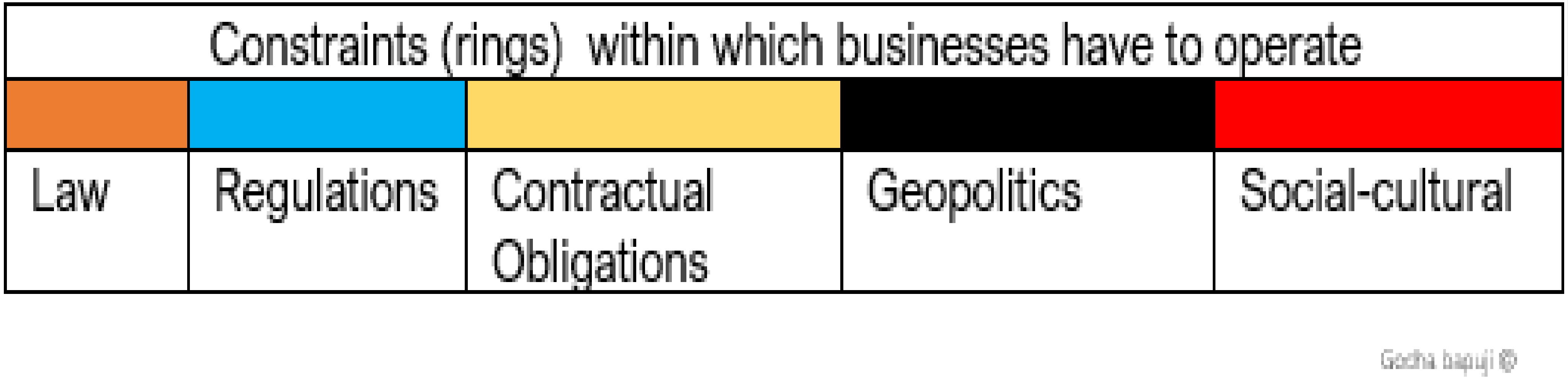
The Four-Fold pattern of Preferences from Thinking Fast and Slow, Kahneman & Tversky, pg 317

Pleasure

	Gains	Losses
High Probability	(e.g. 95% chance to win $10000) Fear of Disappointment	(e.g. 95% chance to lose $10000) Hope to Avoid Loss
Certainity Effect	Risk Averse Accept unfaourable settlement even with high chances of win	Risk Seeking Reject unfaourable settlement even with high chances of losing
Low Probability	(e.g. 5% chance to win $10000) Hopes of Large Gain	(e.g. 5% chance to lose $10000) Fear of Large Loss
Possibility Effect	Risk Seeking Buy Lottery Reject favourable settlement even with high chances of losing	Risk Averse Buy Insurance/Warranties Accept unfavourable settlement even with high chances of win

Pain

But we also work under many limitations



Constraints (rings) within which businesses have to operate				
🟧	🟦	🟨	⬛	🟥
Law	Regulations	Contractual Obligations	Geopolitics	Social-cultural

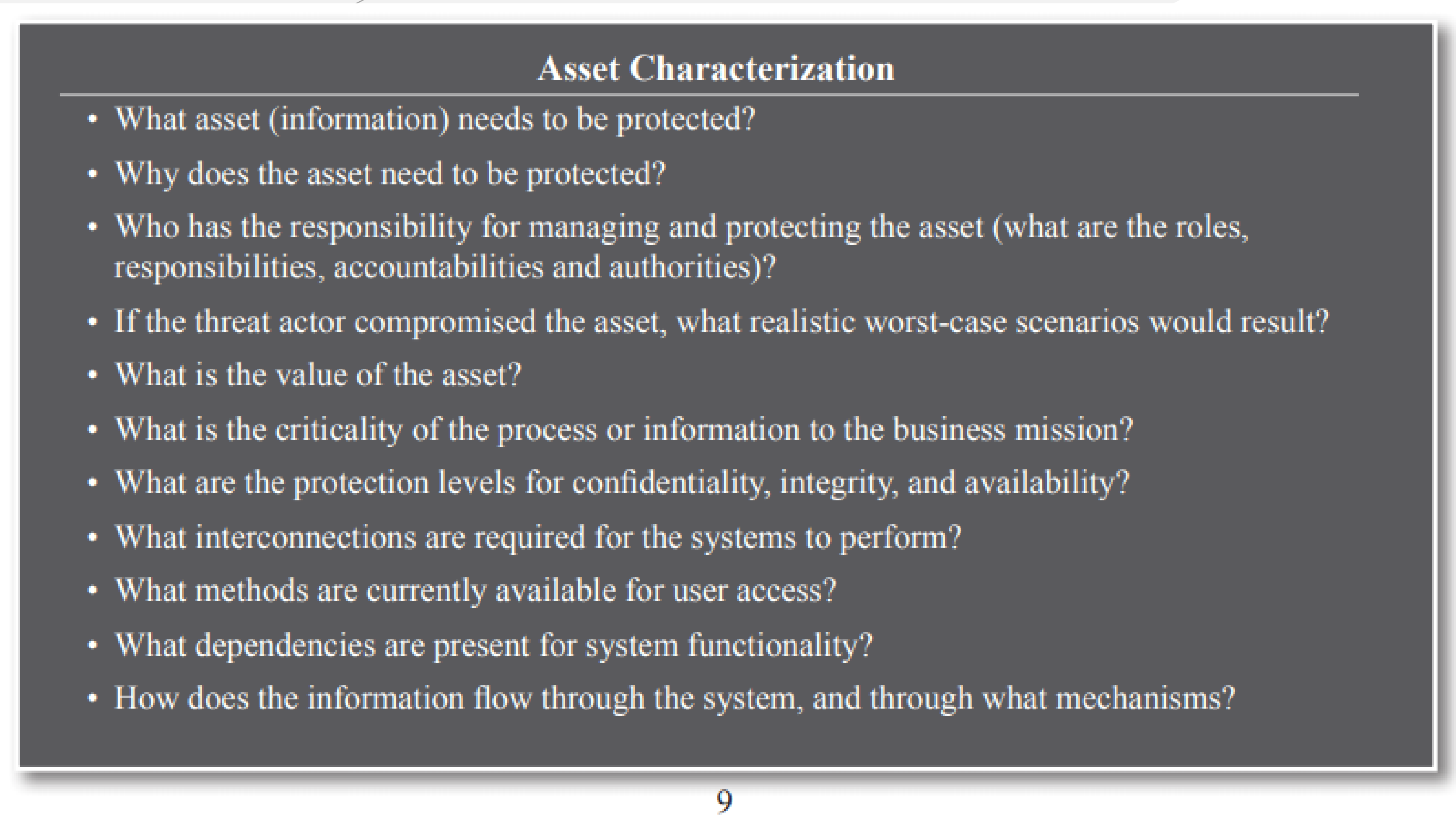
Godha bapuji ©

WiCR
Women must have a place at the table

Preparedness and Capacity Planning

Confidentiality, Integrity, Privacy, Availability, Authentication, Authorisation, Access Control

Understanding the value of what we want to protect



Asset Characterization

- What asset (information) needs to be protected?
- Why does the asset need to be protected?
- Who has the responsibility for managing and protecting the asset (what are the roles, responsibilities, accountabilities and authorities)?
- If the threat actor compromised the asset, what realistic worst-case scenarios would result?
- What is the value of the asset?
- What is the criticality of the process or information to the business mission?
- What are the protection levels for confidentiality, integrity, and availability?
- What interconnections are required for the systems to perform?
- What methods are currently available for user access?
- What dependencies are present for system functionality?
- How does the information flow through the system, and through what mechanisms?

9

https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

WiCR
Women must have a place at the table

Can I help to protect our ICS?

Of Course! You must join in the workforce for the future! Skills required to defend our ICS

Understanding Network Protocols and how they might differ in Industrial systems

Understanding Policies and Safety Regulations in Industrial zones

Understanding how Electrical, Electronics and Mechanical devices work together in Industrial systems

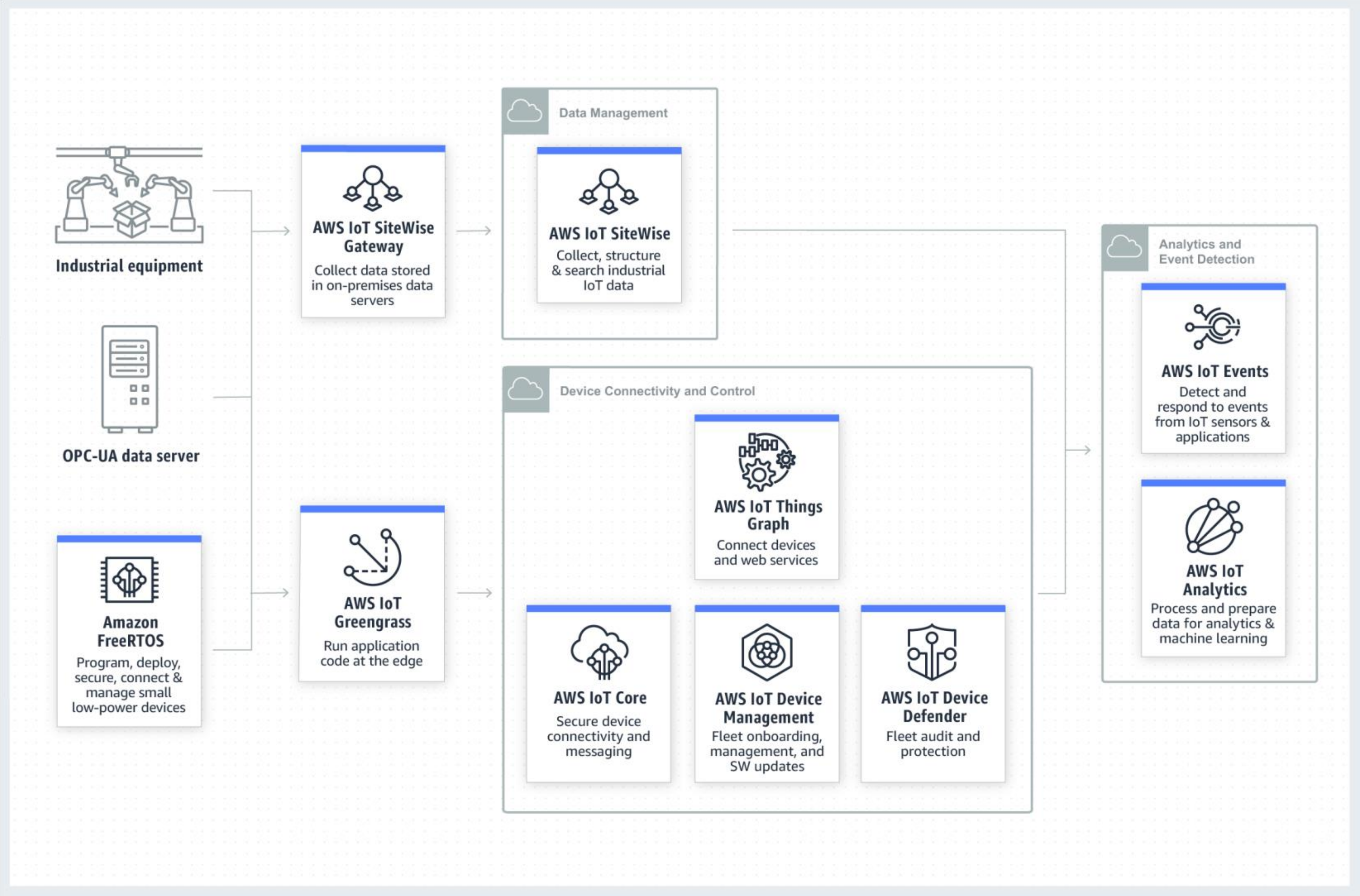
Understanding Risks, Vulnerabilities, threats, and impact on communities due to an industrial system failure

Understanding defenses, Business Continuity and Resilience Needs of each system

Understanding Cultures and Geopolitics of the world

WiCR
Women must have a place at the table

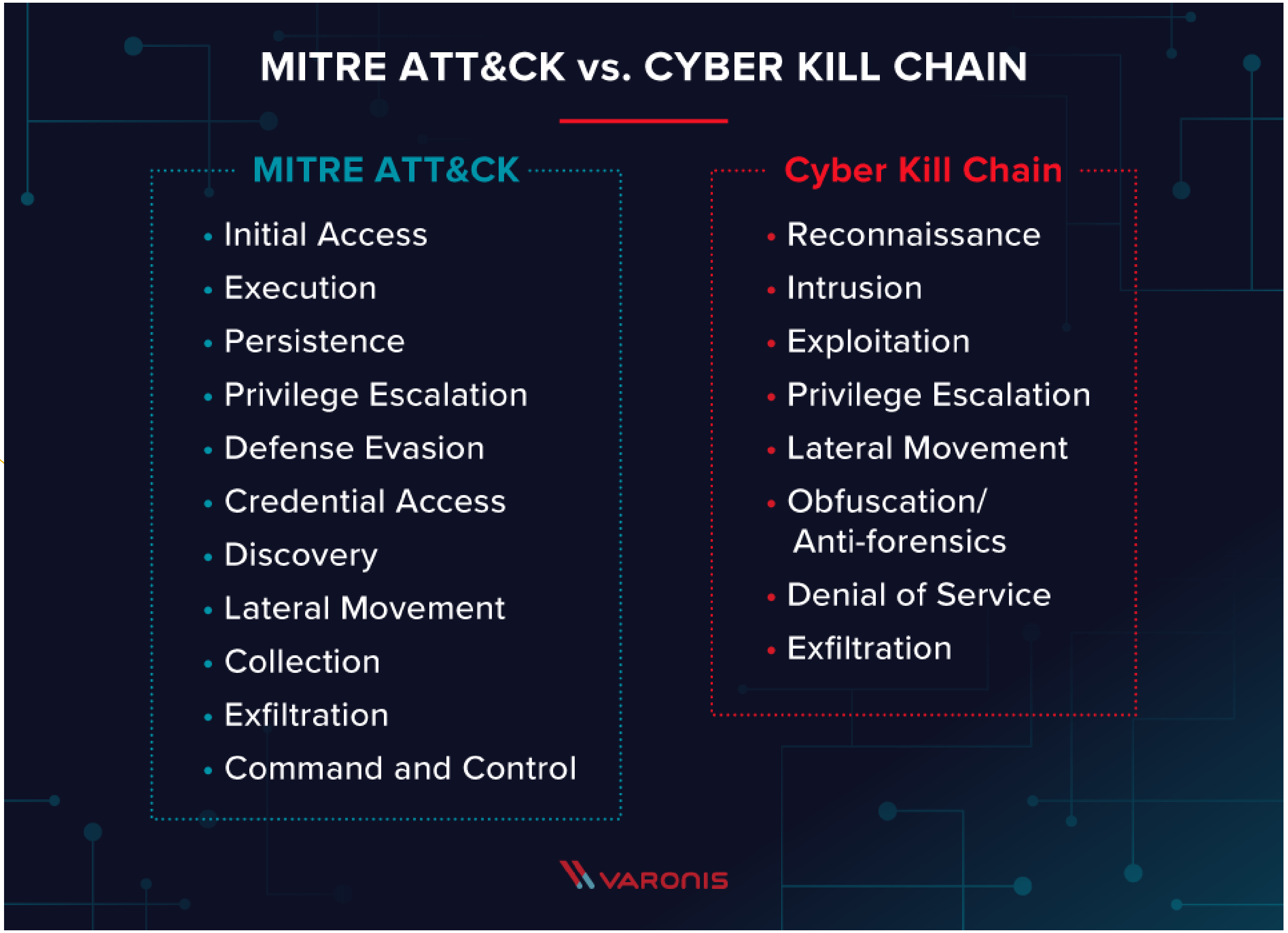
Learn the relevant Cloud services



Industrial equipment
OPC-UA data server
Amazon FreeRTOS
Program, deploy, secure, connect & manage small low-power devices
AWS IoT SiteWise Gateway
Collect data stored in on-premises data servers
AWS IoT Greengrass
Run application code at the edge
Data Management
AWS IoT SiteWise
Collect, structure & search industrial IoT data
Device Connectivity and Control
AWS IoT Things Graph
Connect devices and web services
AWS IoT Core
Secure device connectivity and messaging
AWS IoT Device Management
Fleet onboarding, management, and SW updates
AWS IoT Device Defender
Fleet audit and protection
Analytics and Event Detection
AWS IoT Events
Detect and respond to events from IoT sensors & applications
AWS IoT Analytics
Process and prepare data for analytics & machine learning

https://aws.amazon.com/iot/solutions/industrial-iot/

- Learn MITRE’s threat modeling: a good intro is here:
- https://digitalguardian.com/blog/what-mitre-attck-framework
- Learn about Kill Chains – there are various – start here: https://www.varonis.com/blog/mitre-attck-framework-complete-guide/ and here: https://medium.com/datadriveninvestor/att-ck-model-c40a113aab4



MITRE ATT&CK vs. CYBER KILL CHAIN

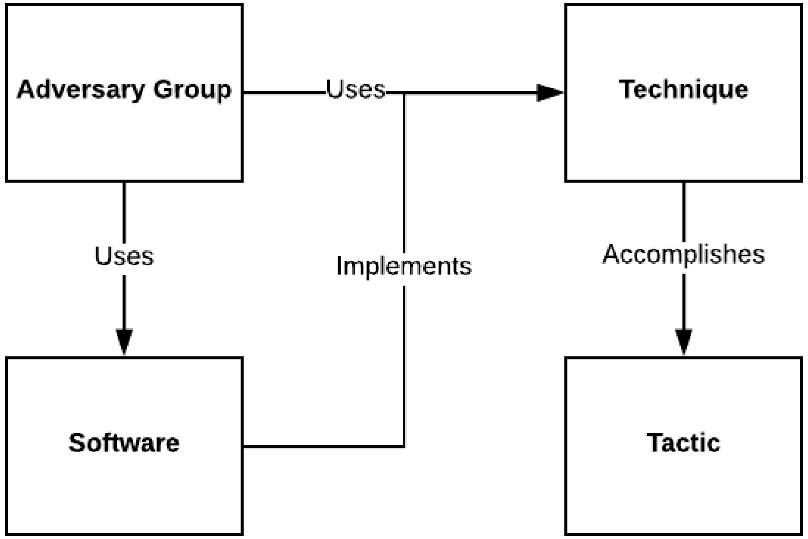
MITRE ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

Cyber Kill Chain

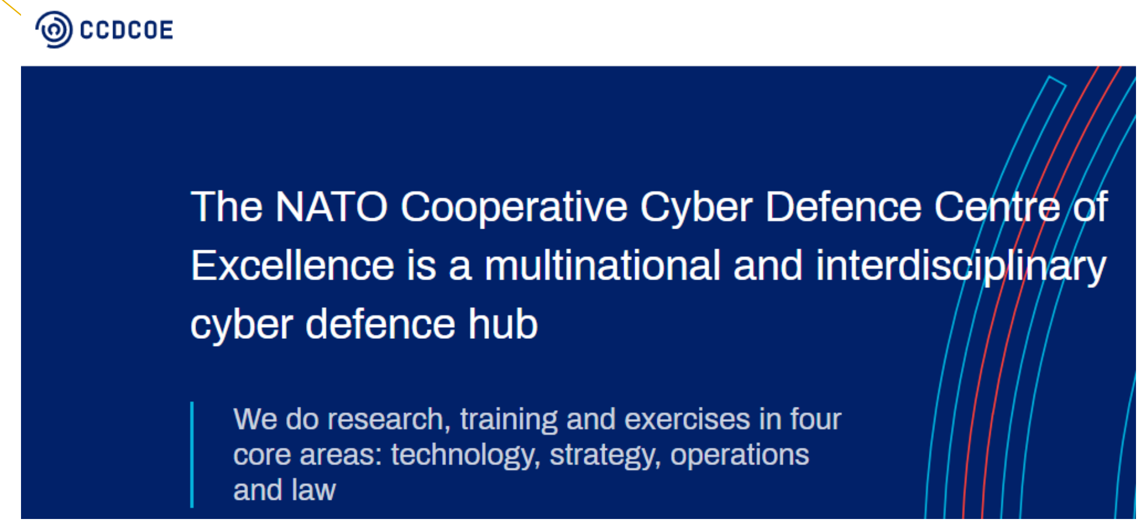
- Reconnaissance
- Intrusion
- Exploitation
- Privilege Escalation
- Lateral Movement
- Obfuscation/ Anti-forensics
- Denial of Service
- Exfiltration

VARONIS



International Relations & International Security

- Take courses in International Relations
- Study how various nations perceive cybersecurity



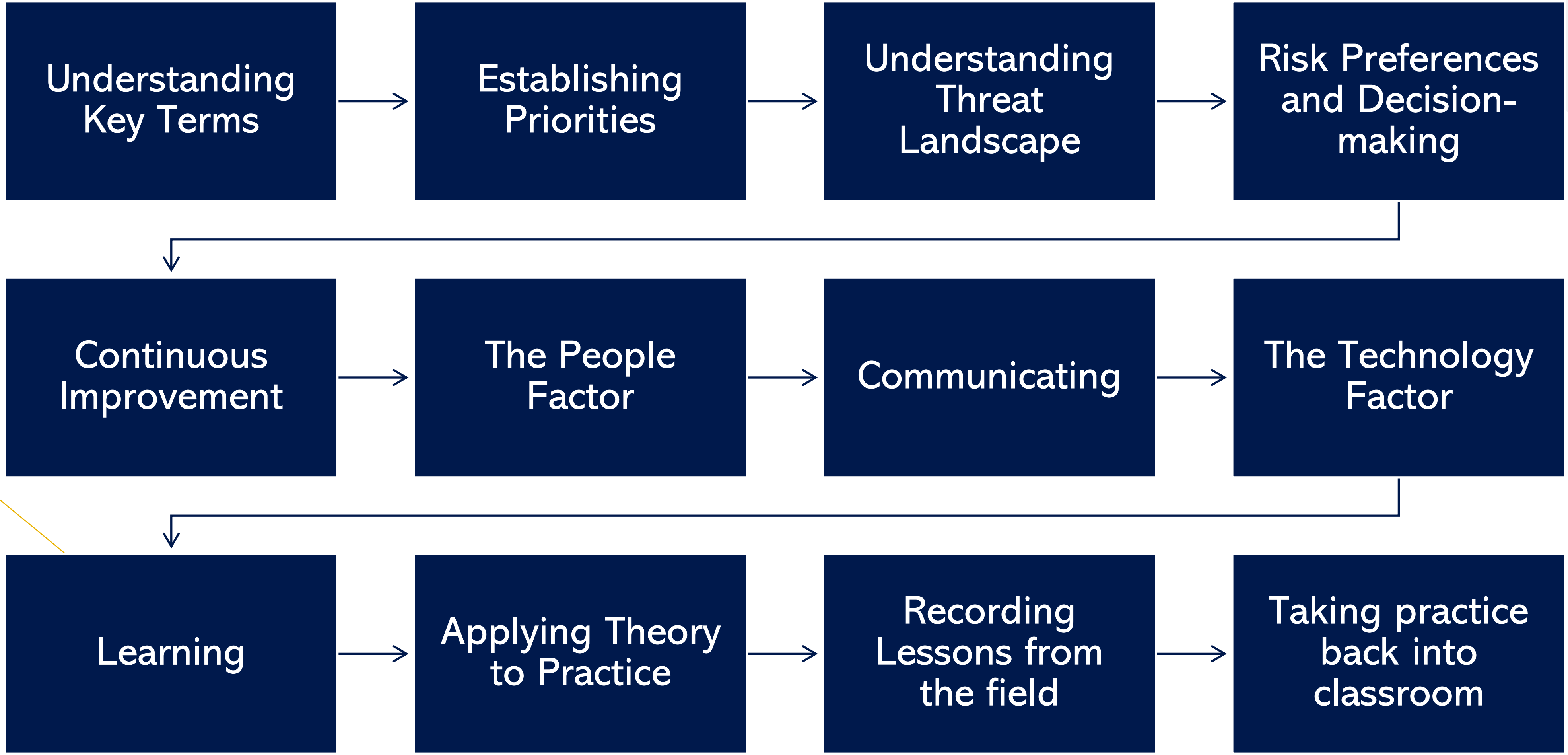
CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub

We do research, training and exercises in four core areas: technology, strategy, operations and law

- Take courses in International Security
- Study what international laws apply to the field of cyber security
- A good place to start would be the NATO website
- The Tallinn 2.0 manual is a great resource to understand cyber laws and other international laws that apply in a cyberspace conflict

A Learning Map



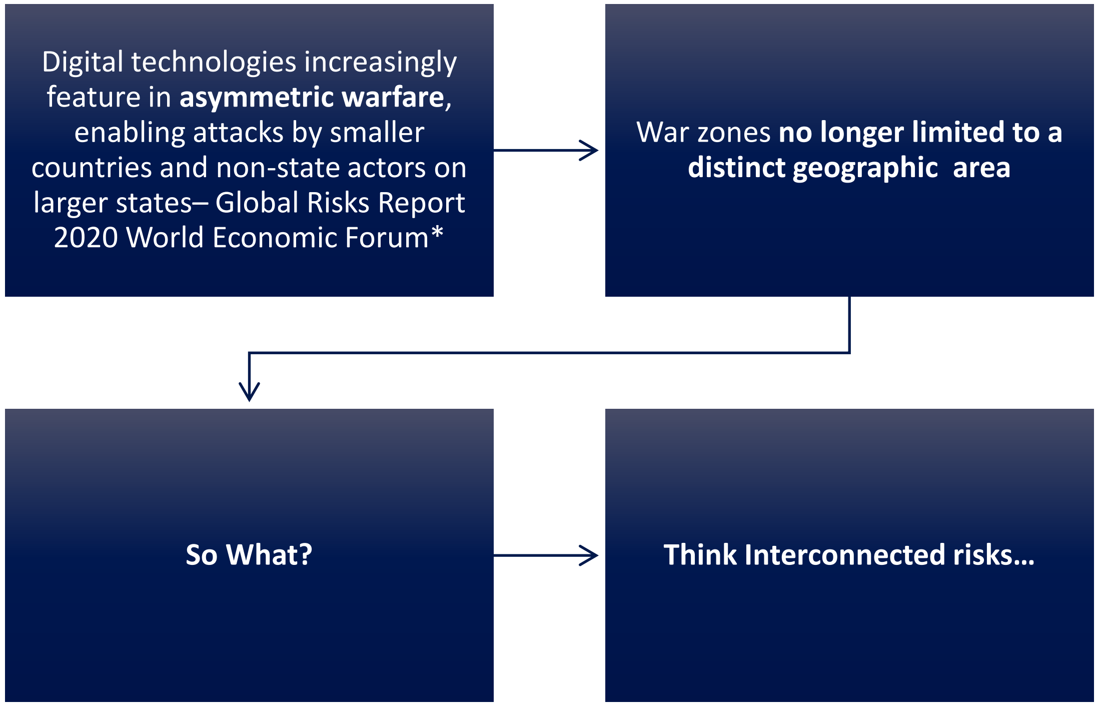
Understanding Key Terms → Establishing Priorities → Understanding Threat Landscape → Risk Preferences and Decision-making

Continuous Improvement → The People Factor → Communicating → The Technology Factor

Learning → Applying Theory to Practice → Recording Lessons from the field → Taking practice back into classroom

Understanding Gaps

How Cybersecurity Gaps lead to Security issues?



Digital technologies increasingly feature in **asymmetric warfare**, enabling attacks by smaller countries and non-state actors on larger states– Global Risks Report 2020 World Economic Forum*

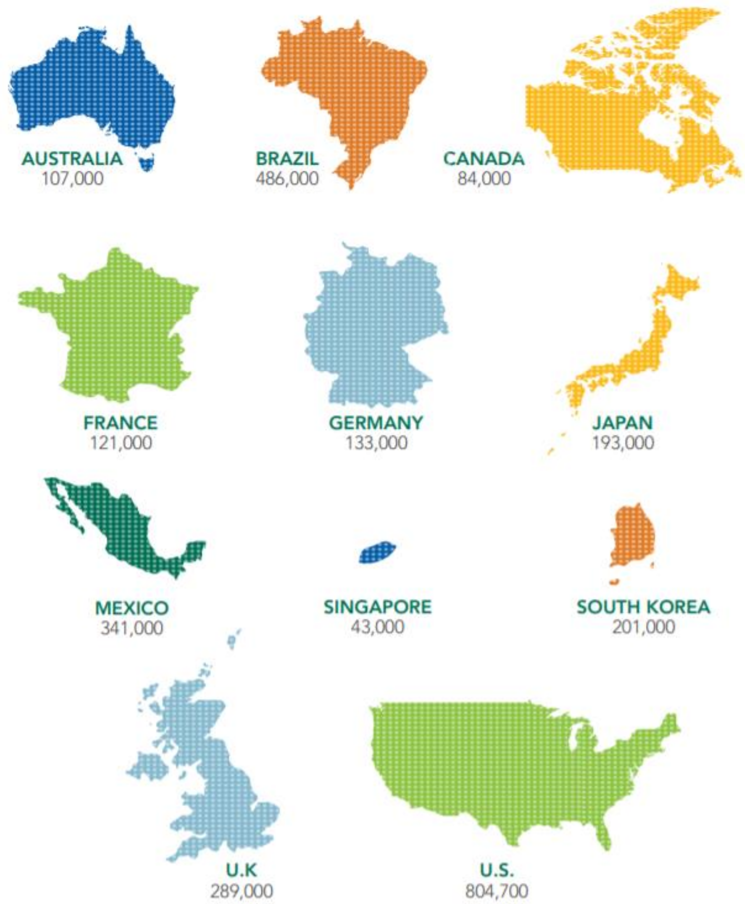
War zones **no longer limited to a distinct geographic area**

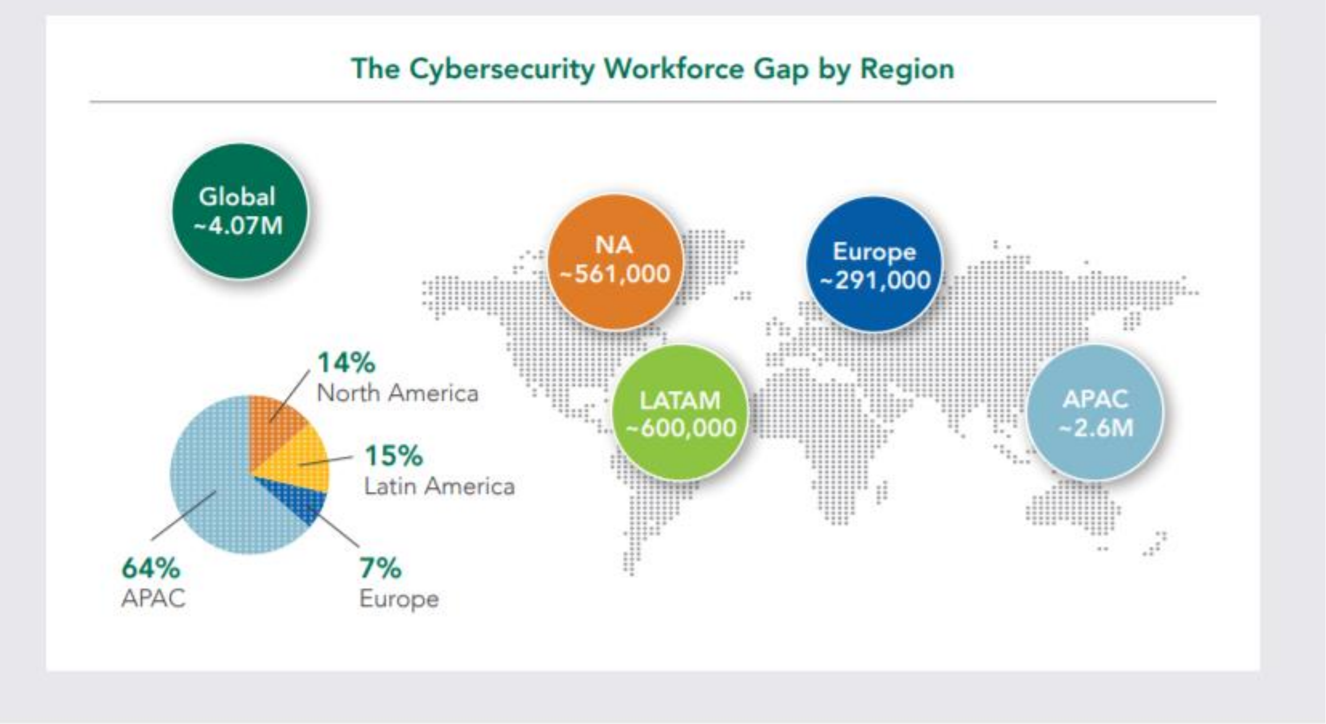
So What?

Think Interconnected risks…

- * Source: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf p5
- ** https://ihl-databases.icrc.org/ihl/385ec082b509e76c41256739003e636d/6756482d86146898c125641e004aa3c5

GLOBAL CYBERSECURITY WORKFORCE ESTIMATES




The Cybersecurity Workforce Gap by Region

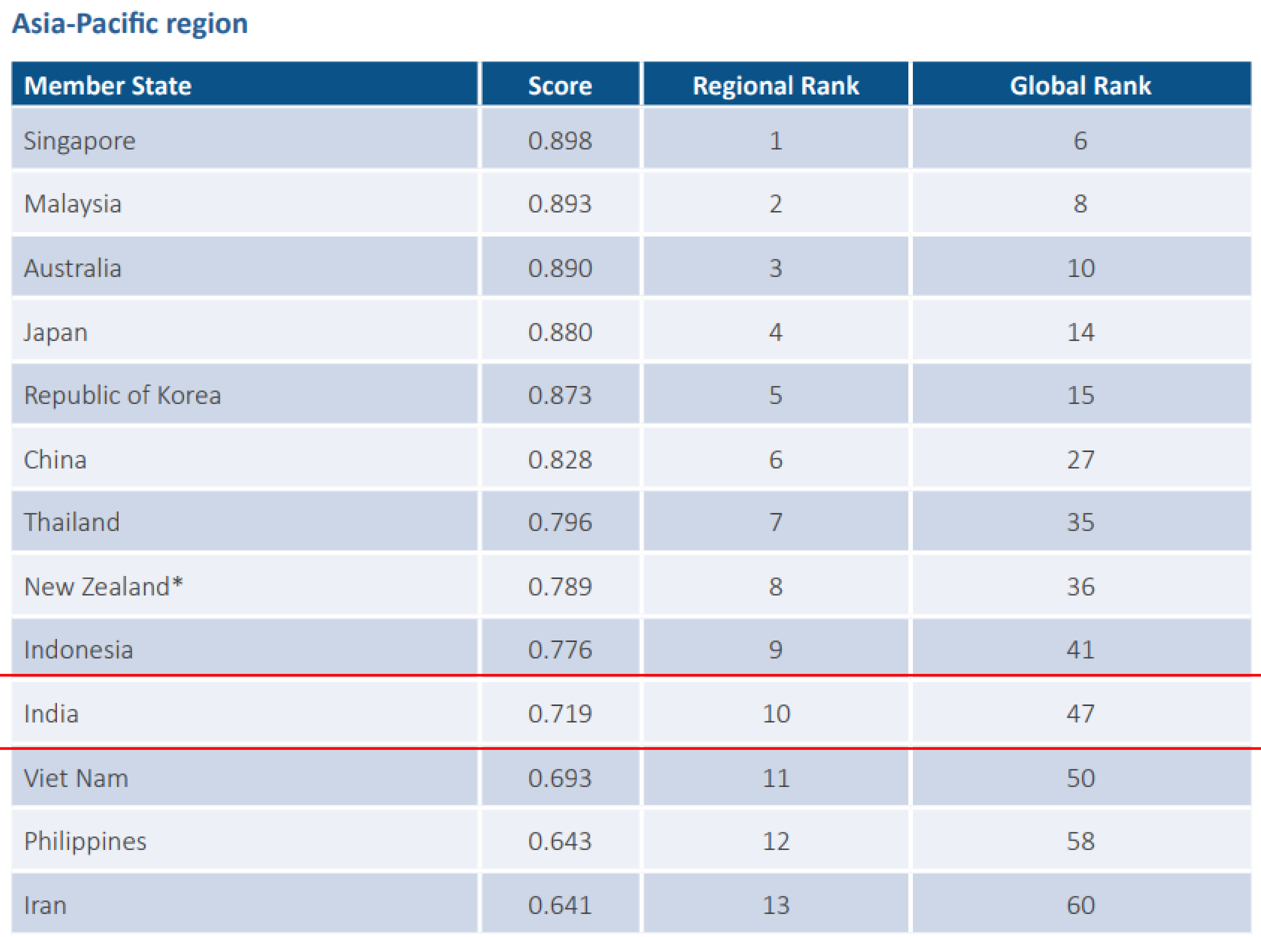
The 2019 ISC2 Cybersecurity Workforce Report shows there aren’t enough people to monitor, prevent, deter, and defend in the cyberspace

And attacks are growing…

See Cybersecurity Workforce Gap on p7, 8

https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

Global Cybersecurity Ranking 2018



Asia-Pacific region

Member State	Score	Regional Rank	Global Rank
Singapore	0.898	1	6
Malaysia	0.893	2	8
Australia	0.890	3	10
Japan	0.880	4	14
Republic of Korea	0.873	5	15
China	0.828	6	27
Thailand	0.796	7	35
New Zealand*	0.789	8	36
Indonesia	0.776	9	41
India	0.719	10	47
Viet Nam	0.693	11	50
Philippines	0.643	12	58
Iran	0.641	13	60

https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

WiCR
Women must have a place at the table

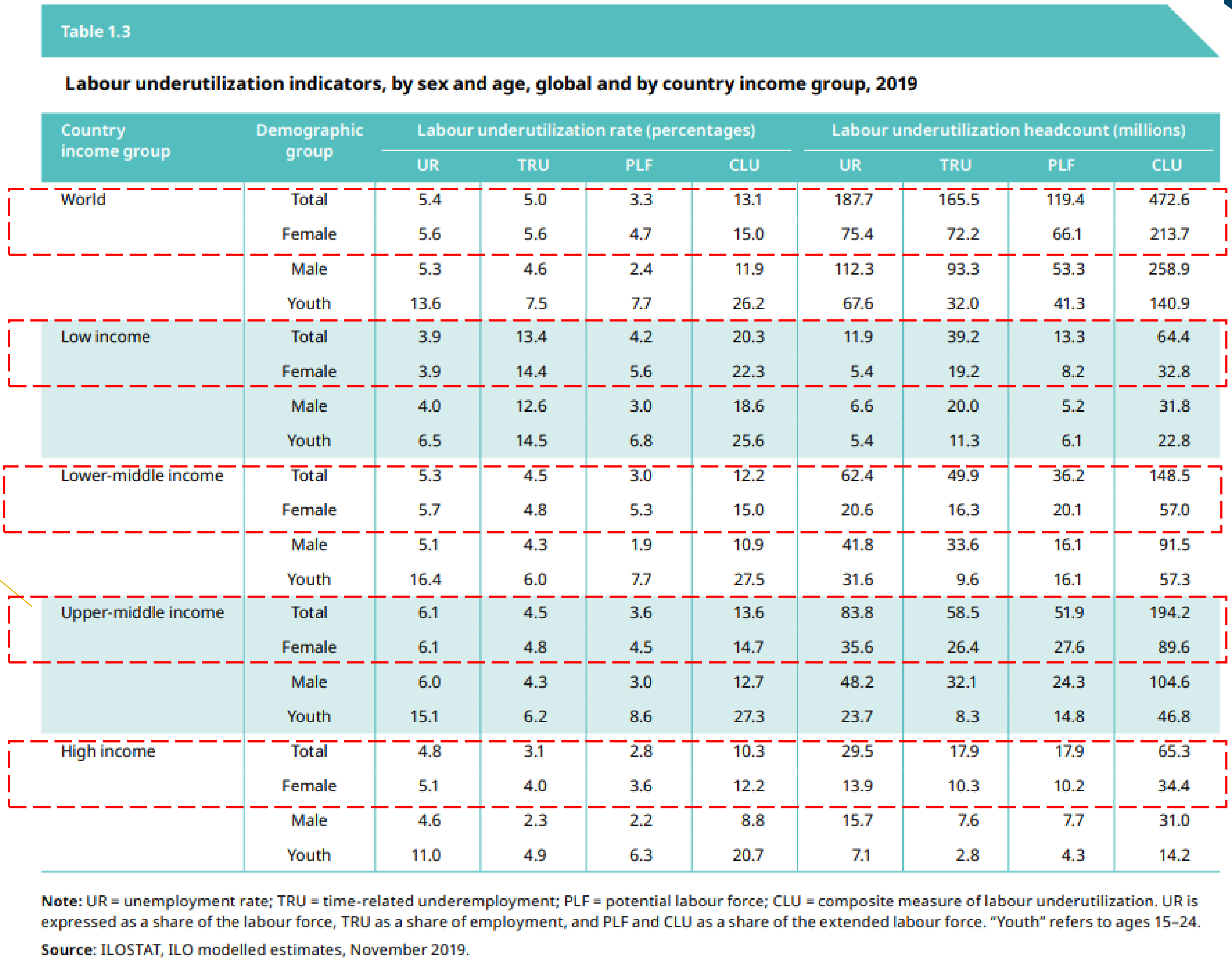


Table 1.3

Labour underutilization indicators, by sex and age, global and by country income group, 2019

Country income group	Demographic group	Labour underutilization rate (percentages)				Labour underutilization headcount (millions)			
		UR	TRU	PLF	CLU	UR	TRU	PLF	CLU
World	Total	5.4	5.0	3.3	13.1	187.7	165.5	119.4	472.6
	Female	5.6	5.6	4.7	15.0	75.4	72.2	66.1	213.7
	Male	5.3	4.6	2.4	11.9	112.3	93.3	53.3	258.9
	Youth	13.6	7.5	7.7	26.2	67.6	32.0	41.3	140.9
Low income	Total	3.9	13.4	4.2	20.3	11.9	39.2	13.3	64.4
	Female	3.9	14.4	5.6	22.3	5.4	19.2	8.2	32.8
	Male	4.0	12.6	3.0	18.6	6.6	20.0	5.2	31.8
	Youth	6.5	14.5	6.8	25.6	5.4	11.3	6.1	22.8
Lower-middle income	Total	5.3	4.5	3.0	12.2	62.4	49.9	36.2	148.5
	Female	5.7	4.8	5.3	15.0	20.6	16.3	20.1	57.0
	Male	5.1	4.3	1.9	10.9	41.8	33.6	16.1	91.5
	Youth	16.4	6.0	7.7	27.5	31.6	9.6	16.1	57.3
Upper-middle income	Total	6.1	4.5	3.6	13.6	83.8	58.5	51.9	194.2
	Female	6.1	4.8	4.5	14.7	35.6	26.4	27.6	89.6
	Male	6.0	4.3	3.0	12.7	48.2	32.1	24.3	104.6
	Youth	15.1	6.2	8.6	27.3	23.7	8.3	14.8	46.8
High income	Total	4.8	3.1	2.8	10.3	29.5	17.9	17.9	65.3
	Female	5.1	4.0	3.6	12.2	13.9	10.3	10.2	34.4
	Male	4.6	2.3	2.2	8.8	15.7	7.6	7.7	31.0
	Youth	11.0	4.9	6.3	20.7	7.1	2.8	4.3	14.2

Note: UR = unemployment rate; TRU = time-related underemployment; PLF = potential labour force; CLU = composite measure of labour underutilization. UR is expressed as a share of the labour force, TRU as a share of employment, and PLF and CLU as a share of the extended labour force. "Youth" refers to ages 15–24.

Source: ILOSTAT, ILO modelled estimates, November 2019.

Potential Labour Force Women vs. Men

- **Female potential labour force is greater** across all income groups compared to men despite barriers to entry and work; there are more qualified or underutilized women in the workforce.
- We **must match** potential to Workforce gap, particularly in Technology and Cybersecurity

But there are barriers

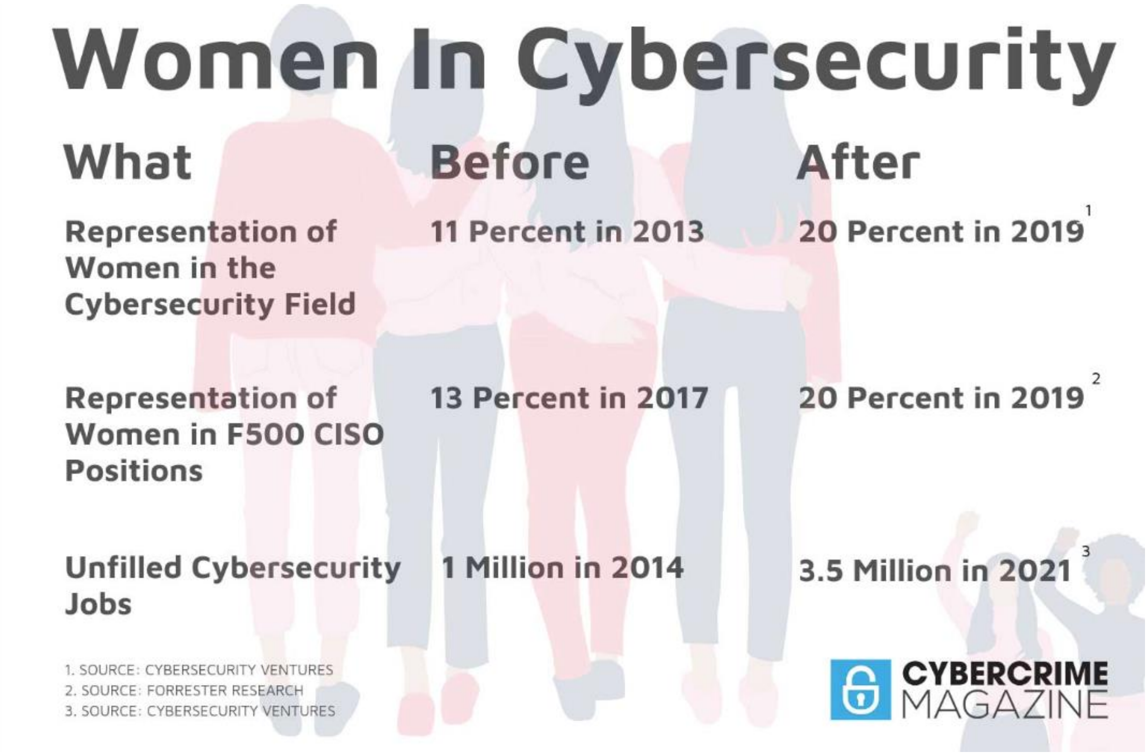
Women in STEM?

Without Women in STEM we will not be able to close the highly skilled workforce gaps today and in the future.

Without Women in STEM we will not be able to mentor women for future Cybersecurity-based positions

See https://www.weforum.org/agenda/2018/02/does-gender-equality-result-in-fewer-female-stem-grads

The Cybersecurity Workforce Current State… improving… but very slowly



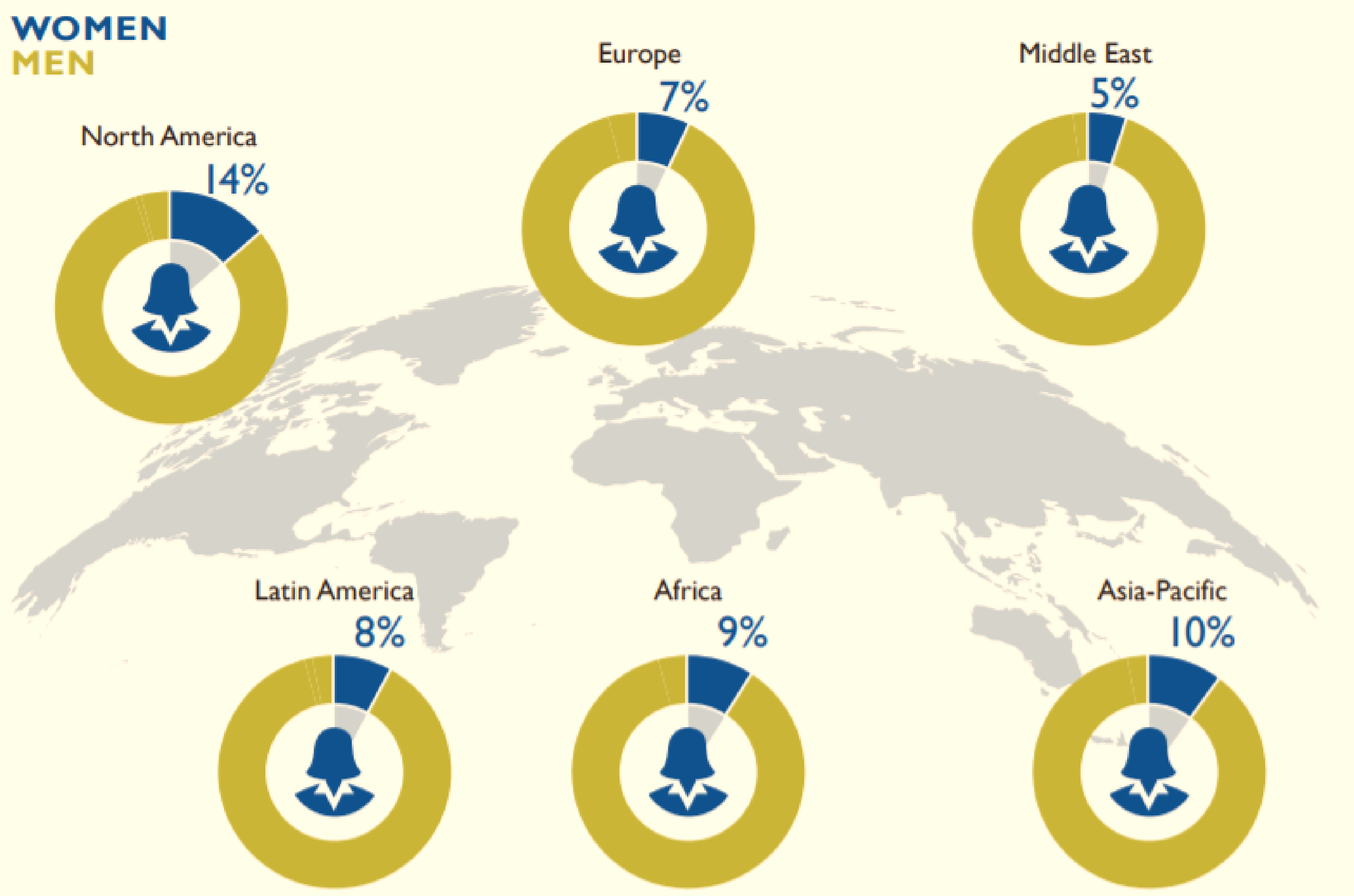
Women In Cybersecurity

What	Before	After
Representation of Women in the Cybersecurity Field	11 Percent in 2013	20 Percent in 2019[1]
Representation of Women in F500 CISO Positions	13 Percent in 2017	20 Percent in 2019[2]
Unfilled Cybersecurity Jobs	1 Million in 2014	3.5 Million in 2021[3]

1. SOURCE: CYBERSECURITY VENTURES
2. SOURCE: FORRESTER RESEARCH
3. SOURCE: CYBERSECURITY VENTURES

CYBERCRIME MAGAZINE

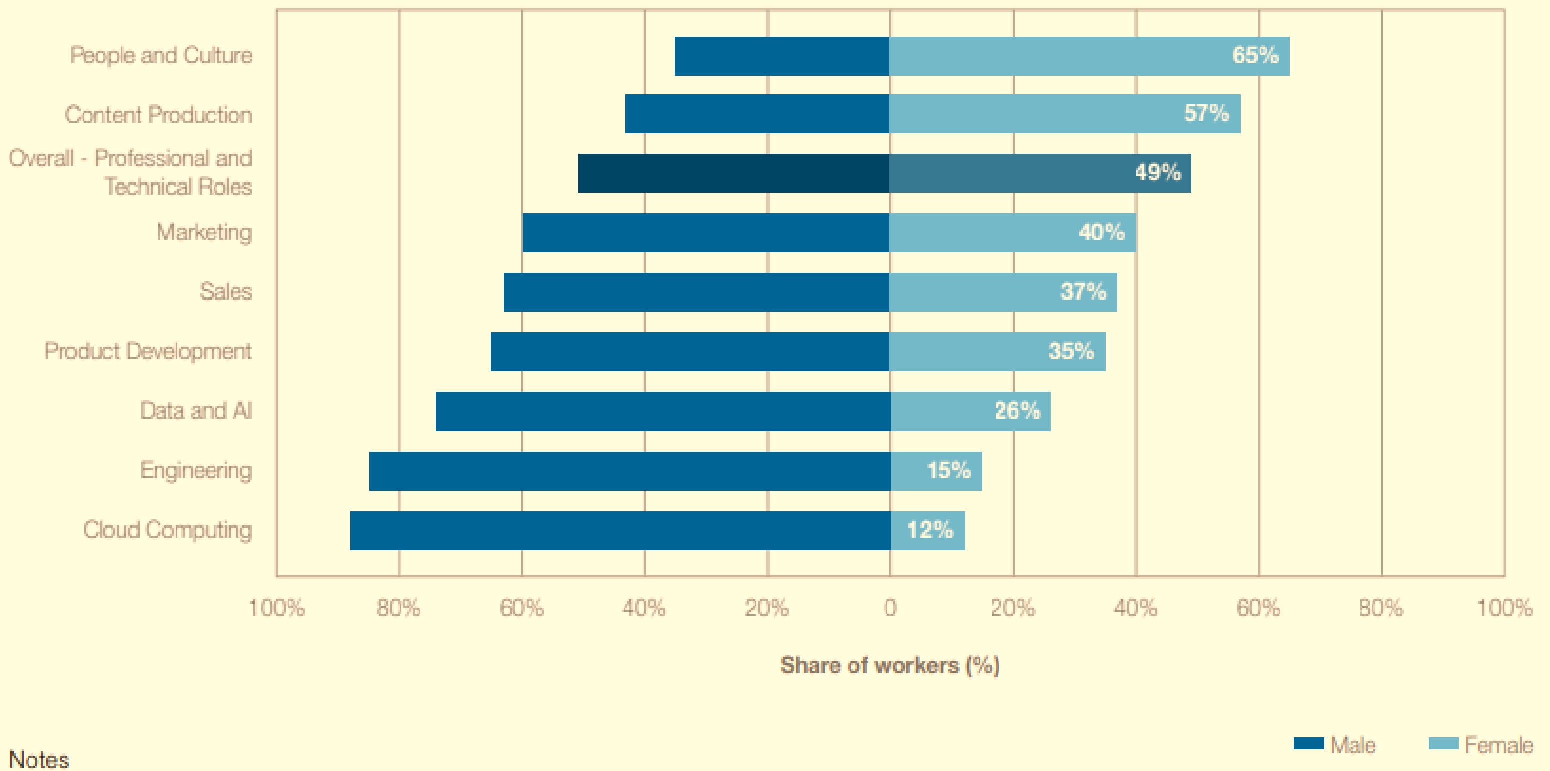
Exhibit #1: Male and Female Cybersecurity Workforce Composition, by Region



Source: 2017 Global Information Security Workforce Study, (n=19,641)

Male vs female cybersecurity workforce composition

Figure 1 Share of male and female workers across professional clusters

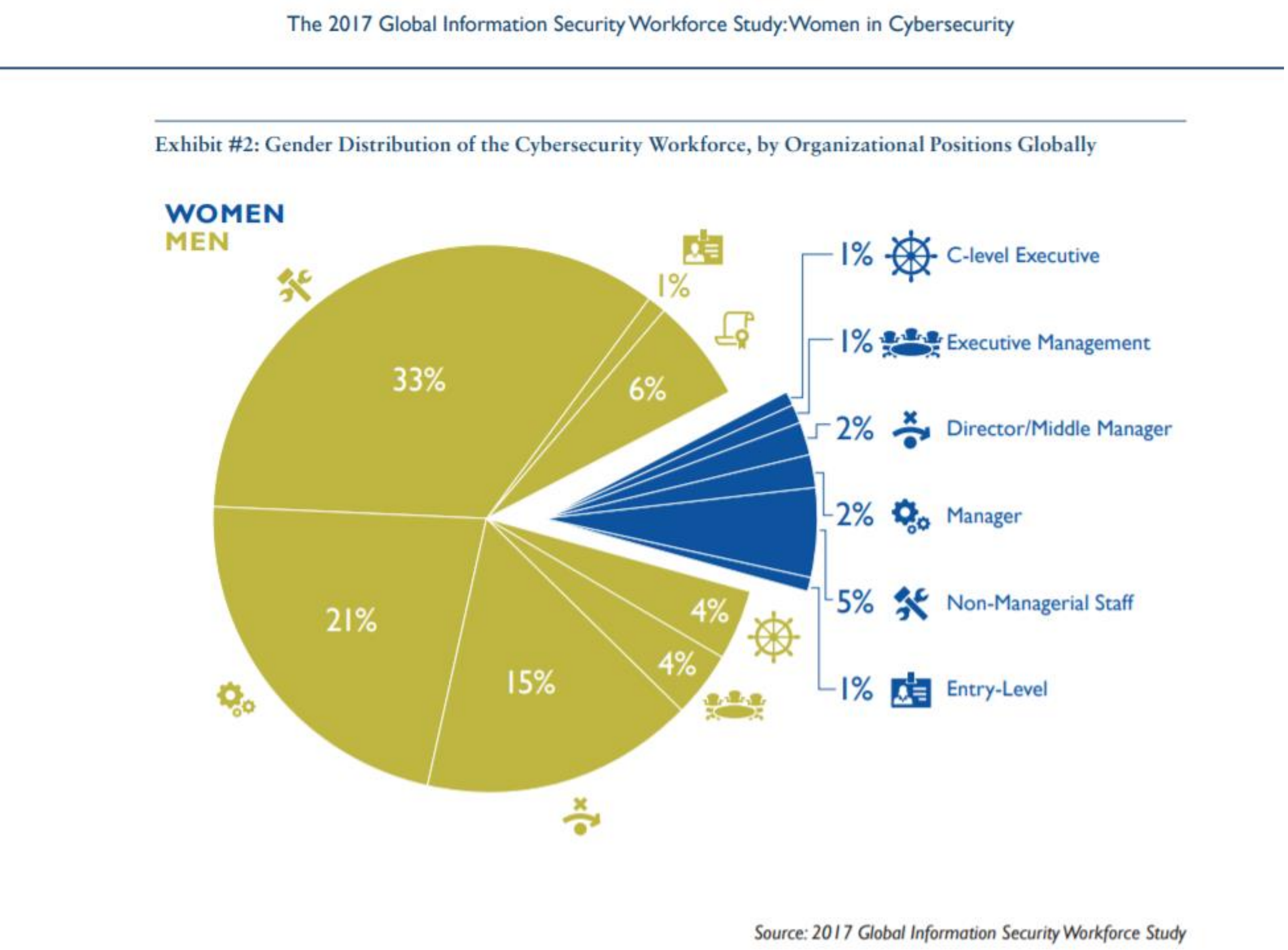


Notes

All data except for "General – Professional and Technical Roles" is sourced from LinkedIn. The additional data point is provided for context and sourced from ILO.

- Only 2 of the 8 groups show greater women to men ratio – People and Culture and Content Production.

See World Economic Forum Gender Gap Report 2020 p37: http://www3.weforum.org/docs/WEF_GGGR_2020.pdf



The 2017 Global Information Security Workforce Study: Women in Cybersecurity

Exhibit #2: Gender Distribution of the Cybersecurity Workforce, by Organizational Positions Globally

Source: 2017 Global Information Security Workforce Study

Disproportional sharing of roles

- Many job roles can be shared more evenly with women but are not!
- With more cyber security positions filled by women, we can backfill the cybersecurity workforce gap

But there are challenges such as discrimination…

see pages 7 and 13

The Cybersecurity Workforce Gender Issues: Forms of discrimination

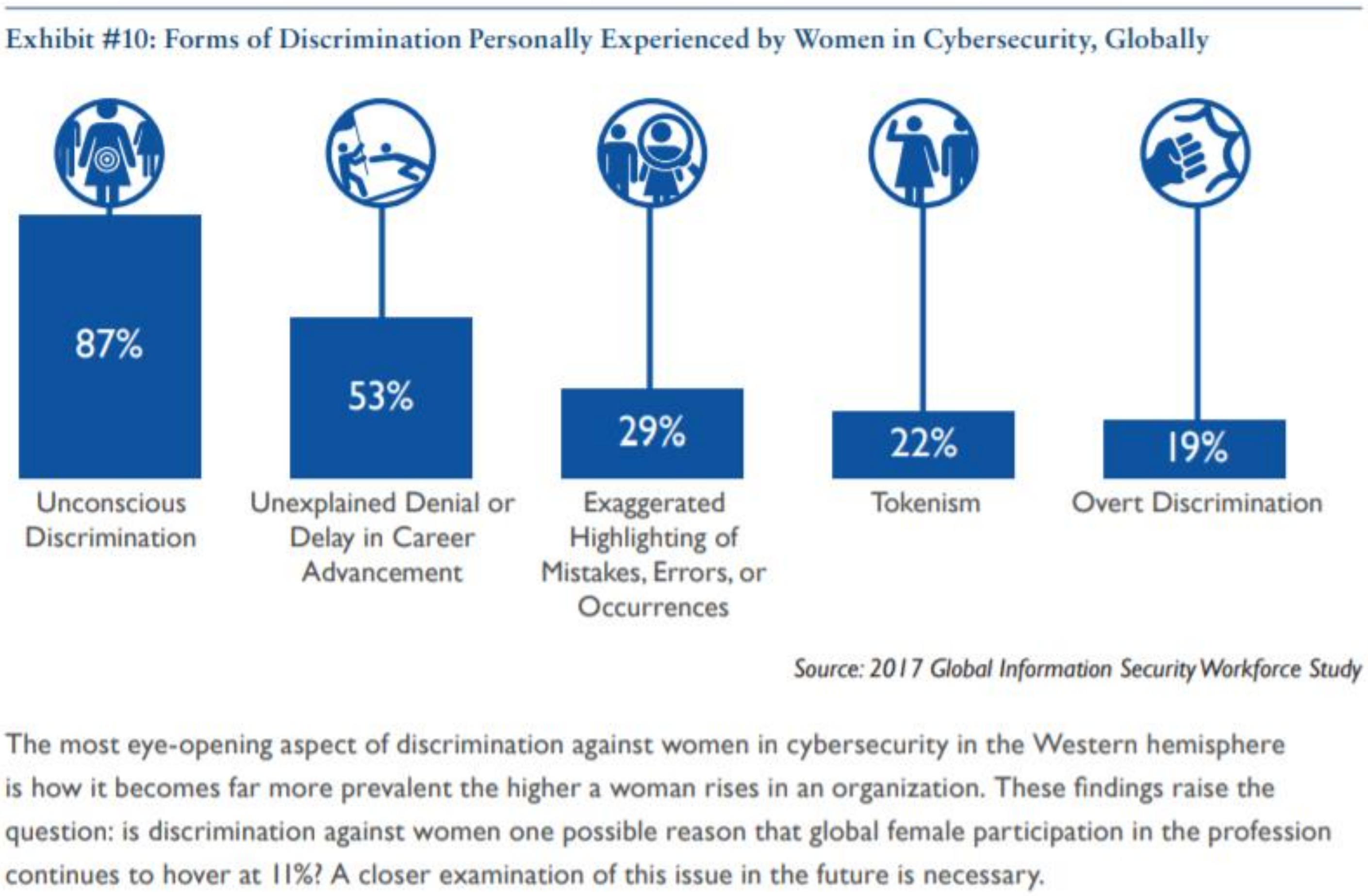


Exhibit #10: Forms of Discrimination Personally Experienced by Women in Cybersecurity, Globally

Source: 2017 Global Information Security Workforce Study

The most eye-opening aspect of discrimination against women in cybersecurity in the Western hemisphere is how it becomes far more prevalent the higher a woman rises in an organization. These findings raise the question: is discrimination against women one possible reason that global female participation in the profession continues to hover at 11%? A closer examination of this issue in the future is necessary.

2017 Global Information Security Workforce Study: Women in Cybersecurity see pages 7 and 13

WiCR
Women must have a place at the table

Women can help tackle this growing challenge of attacks on our societies.

Women workforce today is either underutilized or unemployed due to many socio-cultural barriers

Growing Attacks and comparatively fewer defenses is under preparation and is a Threat to National and International Security

Appendix

WiCR
Women must have a place at the table

Five terms to know well

- SCADA
- Distributed control system (DCS)
- Programmable logic controller (PLC)
- Remote terminal unit (RTU) and
- Smart instrument

https://electrical-engineering-portal.com/scada-dcs-plc-rtu-smart-instrument

WiCR
Women must have a place at the table

SCADA (Supervisory Control and Data Acquisition)

These systems are used in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical utility transmission and distribution systems, and rail and other public transportation systems.

SCADA systems integrate data acquisition systems with data transmission systems and HMI software to provide a centralized monitoring and control system for numerous process inputs and outputs.

SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in near real time.

Based on the sophistication and setup of the individual system, control of any individual system, operation, or task can be automatic, or it can be performed by operator commands.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

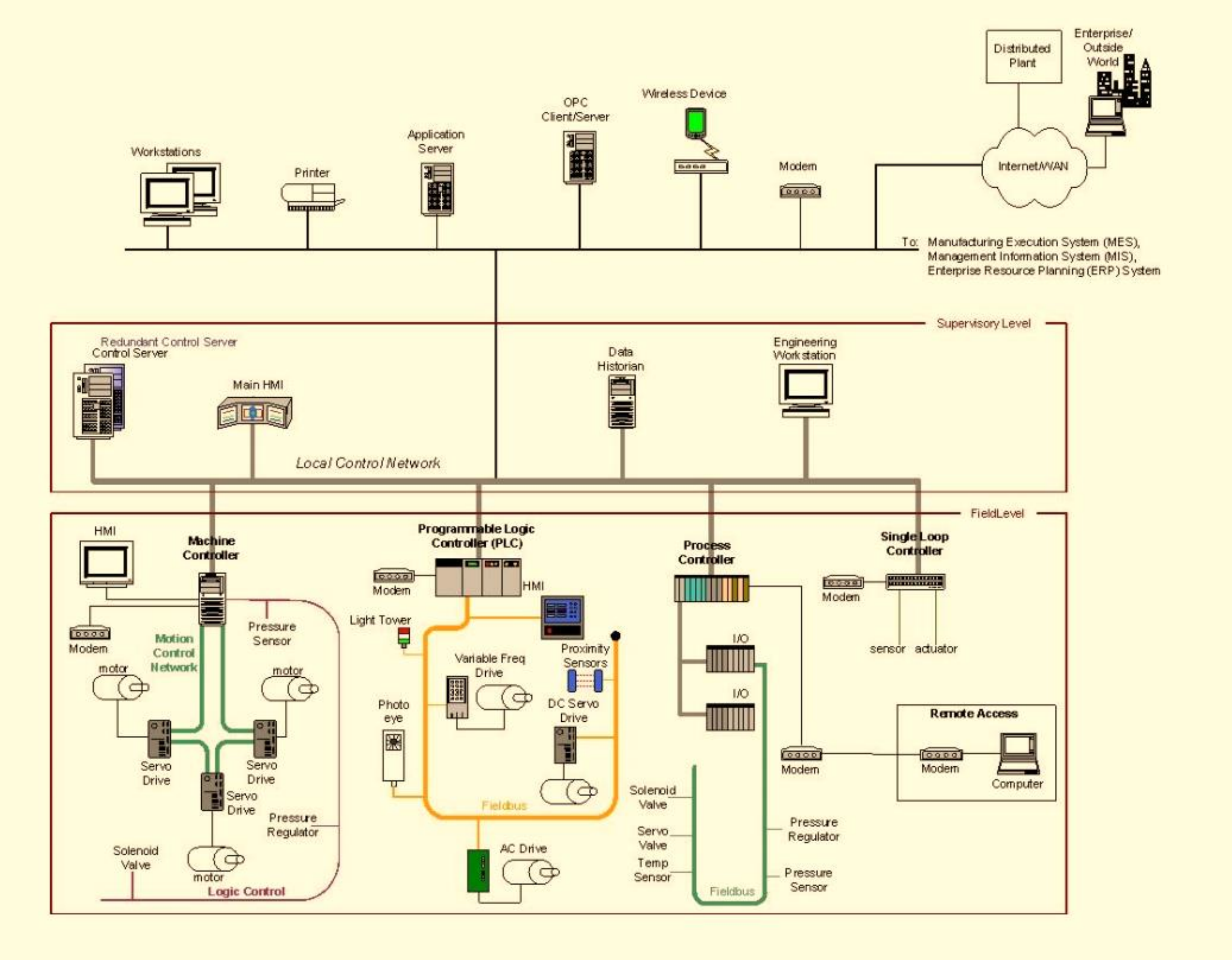


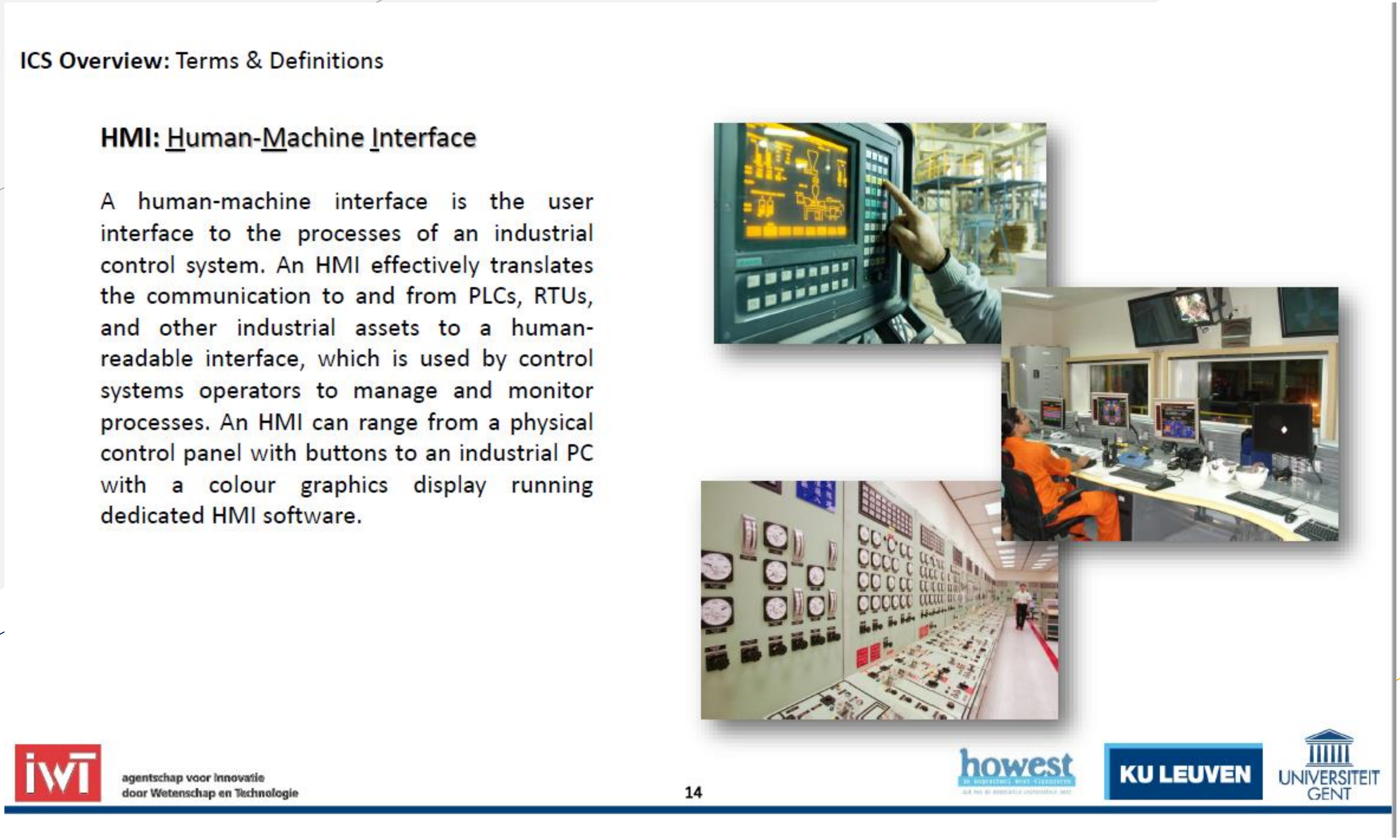
Figure 2-7. DCS Implementation Example

Distributed Control Systems (DCS)

- DCS are used to control production systems within the same geographic location for industries such as oil refineries, water and wastewater treatment, electric power generation plants, chemical manufacturing plants, automotive production, and pharmaceutical processing facilities.
- Typical control devices include Programmable Logic Controller, a Process Controller, a loop controller, a machine controller

Stouffer, Keith & Falco, Joseph & Kent, Karen. (2006). Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security.

A great intro deck



ICS Overview: Terms & Definitions

HMI: Human-Machine Interface

A human-machine interface is the user interface to the processes of an industrial control system. An HMI effectively translates the communication to and from PLCs, RTUs, and other industrial assets to a human-readable interface, which is used by control systems operators to manage and monitor processes. An HMI can range from a physical control panel with buttons to an industrial PC with a colour graphics display running dedicated HMI software.

iwt agentschap voor Innovatie door Wetenschap en Technologie

14

howest KU LEUVEN UNIVERSITEIT GENT

https://www.msec.be/verboten/seminaries/ICS_archs_and_sec_essentials/ICS_Overview.pdf

What is the 4th Industrial Revolution and how does it matter?

Cyber-Physical

NIST defines this as: “*Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic.”*

See NIST Special Publication 1500-201 for more details on CPS. *

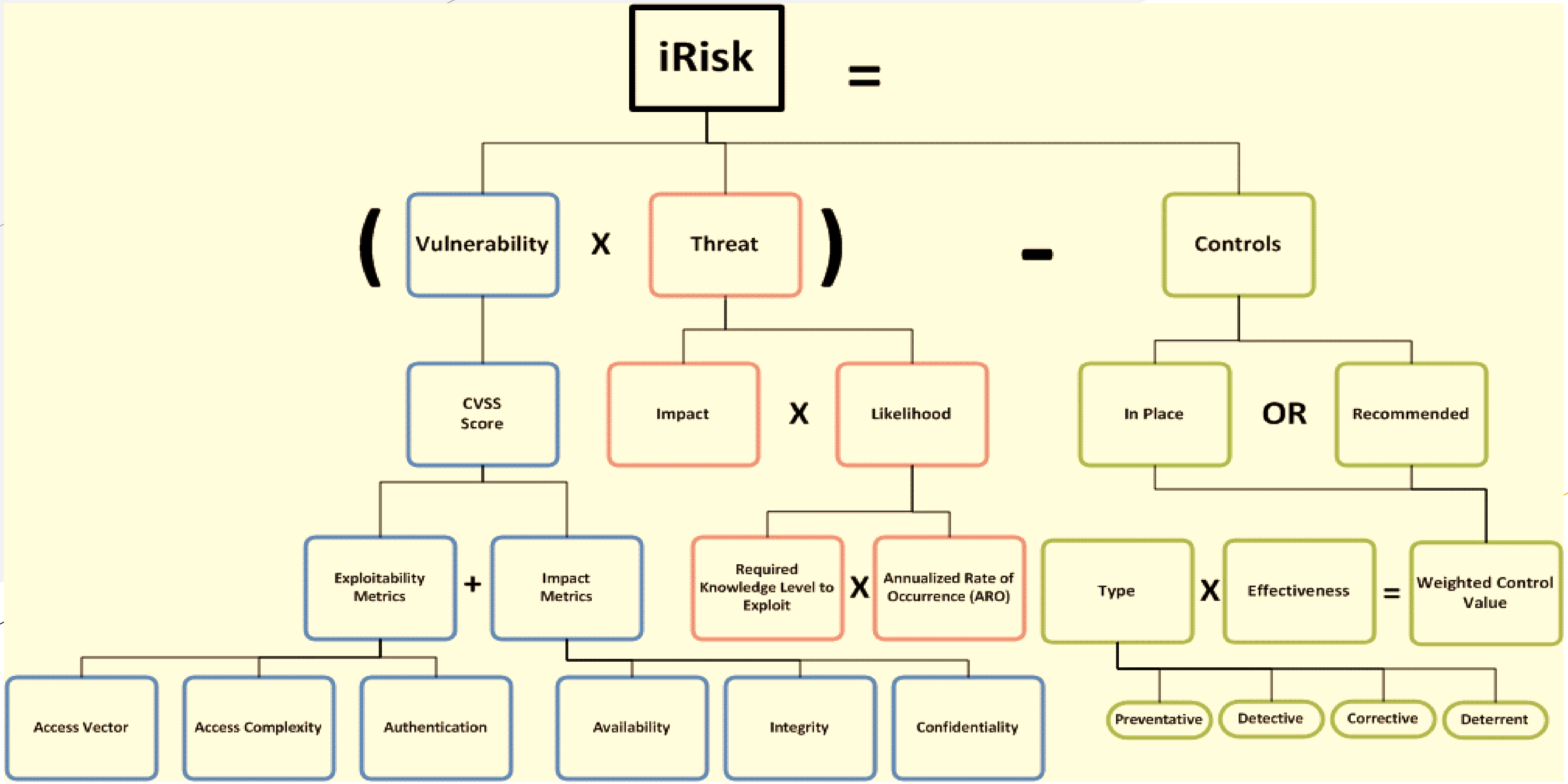
Internet of Things

Cloud-enabled electromechanical components can now beam continuous data not just about their status and wellbeing but also about the various parameters of inputs and output data.

* https://www.nist.gov/el/cyber-physical-systems

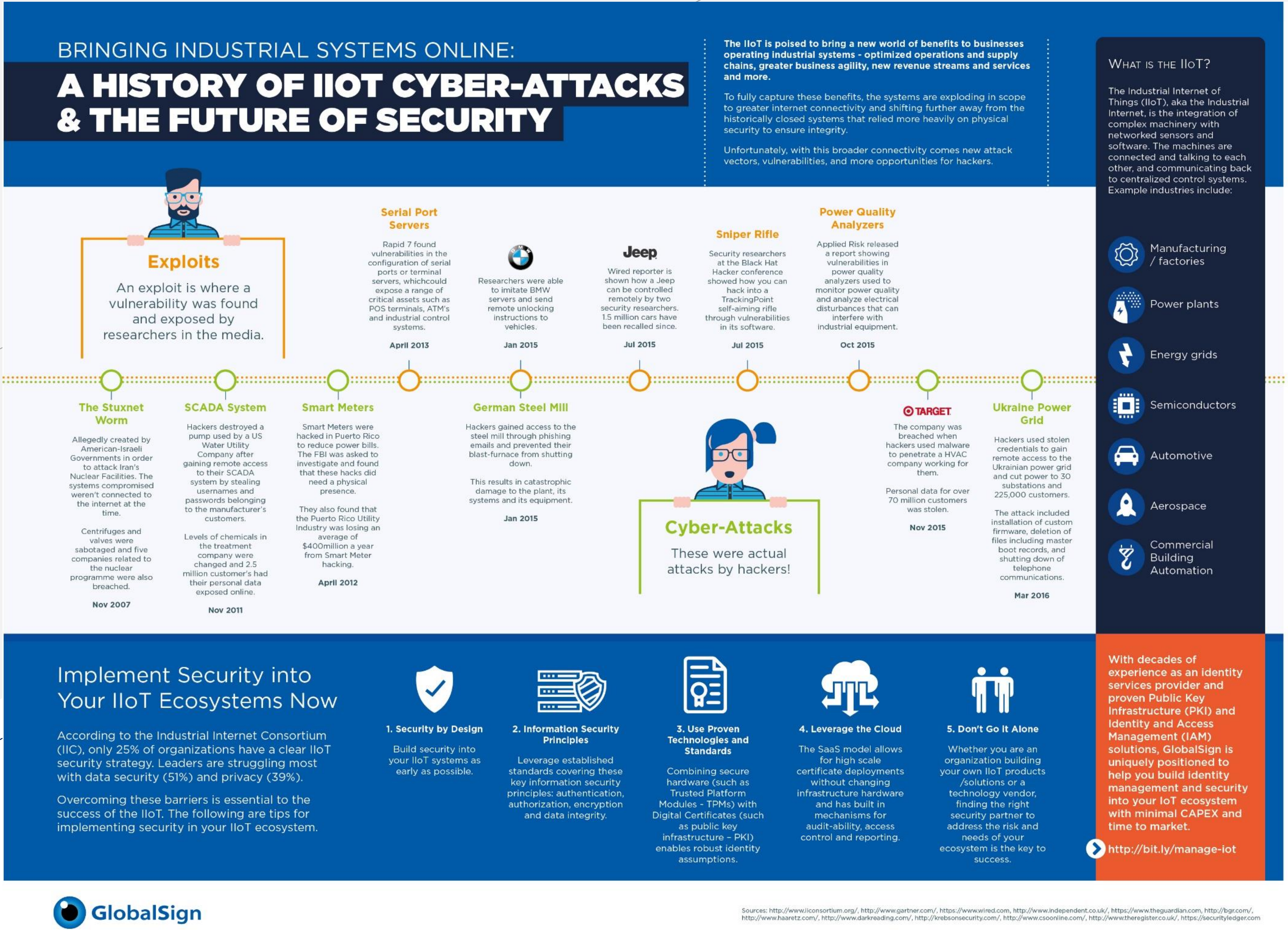
Measuring Risk

WiCR
Women must have a place at the table



https://www.carmelowalsh.com/wp-content/uploads/2014/03/Irisk_full_web.png

Some well-known cyber attacks on industrial systems



BRINGING INDUSTRIAL SYSTEMS ONLINE:

A HISTORY OF IIOT CYBER-ATTACKS & THE FUTURE OF SECURITY

The IIoT is poised to bring a new world of benefits to businesses operating industrial systems - optimized operations and supply chains, greater business agility, new revenue streams and services and more.

To fully capture these benefits, the systems are exploding in scope to greater internet connectivity and shifting further away from the historically closed systems that relied more heavily on physical security to ensure integrity.

Unfortunately, with this broader connectivity comes new attack vectors, vulnerabilities, and more opportunities for hackers.

What is the IIoT?

The Industrial Internet of Things (IIoT), aka the Industrial Internet, is the integration of complex machinery with networked sensors and software. The machines are connected and talking to each other, and communicating back to centralized control systems. Example industries include:

- Manufacturing / factories
- Power plants
- Energy grids
- Semiconductors
- Automotive
- Aerospace
- Commercial Building Automation

Exploits

An exploit is where a vulnerability was found and exposed by researchers in the media.

Serial Port Servers

Rapid 7 found vulnerabilities in the configuration of serial ports or terminal servers, whichcould expose a range of critical assets such as POS terminals, ATM's and industrial control systems.

April 2013

BMW

Researchers were able to imitate BMW servers and send remote unlocking instructions to vehicles.

Jan 2015

Jeep

Wired reporter is shown how a Jeep can be controlled remotely by two security researchers. 1.5 million cars have been recalled since.

Jul 2015

Sniper Rifle

Security researchers at the Black Hat Hacker conference showed how you can hack into a TrackingPoint self-aiming rifle through vulnerabilities in its software.

Jul 2015

Power Quality Analyzers

Applied Risk released a report showing vulnerabilities in power quality analyzers used to monitor power quality and analyze electrical disturbances that can interfere with industrial equipment.

Oct 2015

Cyber-Attacks

These were actual attacks by hackers!

The Stuxnet Worm

Allegedly created by American-Israeli Governments in order to attack Iran's Nuclear Facilities. The systems compromised weren't connected to the internet at the time.

Centrifuges and valves were sabotaged and five companies related to the nuclear programme were also breached.

Nov 2007

SCADA System

Hackers destroyed a pump used by a US Water Utility Company after gaining remote access to their SCADA system by stealing usernames and passwords belonging to the manufacturer's customers.

Levels of chemicals in the treatment company were changed and 2.5 million customer's had their personal data exposed online.

Nov 2011

Smart Meters

Smart Meters were hacked in Puerto Rico to reduce power bills. The FBI was asked to investigate and found that these hacks did need a physical presence.

They also found that the Puerto Rico Utility Industry was losing an average of $400million a year from Smart Meter hacking.

April 2012

German Steel Mill

Hackers gained access to the steel mill through phishing emails and prevented their blast-furnace from shutting down.

This results in catastrophic damage to the plant, its systems and its equipment.

Jan 2015

TARGET

The company was breached when hackers used malware to penetrate a HVAC company working for them.

Personal data for over 70 million customers was stolen.

Nov 2015

Ukraine Power Grid

Hackers used stolen credentials to gain remote access to the Ukrainian power grid and cut power to 30 substations and 225,000 customers.

The attack included installation of custom firmware, deletion of files including master boot records, and shutting down of telephone communications.

Mar 2016

Implement Security into Your IIoT Ecosystems Now

According to the Industrial Internet Consortium (IIC), only 25% of organizations have a clear IIoT security strategy. Leaders are struggling most with data security (51%) and privacy (39%).

Overcoming these barriers is essential to the success of the IIoT. The following are tips for implementing security in your IIoT ecosystem.

1. Security by Design

Build security into your IIoT systems as early as possible.

2. Information Security Principles

Leverage established standards covering these key information security principles: authentication, authorization, encryption and data integrity.

3. Use Proven Technologies and Standards

Combining secure hardware (such as Trusted Platform Modules - TPMs) with Digital Certificates (such as public key infrastructure - PKI) enables robust identity assumptions.

4. Leverage the Cloud

The SaaS model allows for high scale certificate deployments without changing infrastructure hardware and has built in mechanisms for audit-ability, access control and reporting.

5. Don't Go It Alone

Whether you are an organization building your own IIoT products /solutions or a technology vendor, finding the right security partner to address the risk and needs of your ecosystem is the key to success.

With decades of experience as an identity services provider and proven Public Key Infrastructure (PKI) and Identity and Access Management (IAM) solutions, GlobalSign is uniquely positioned to help you build identity management and security into your IoT ecosystem with minimal CAPEX and time to market.

http://bit.ly/manage-iot

GlobalSign

Sources: http://www.iiconsortium.org/, http://www.gartner.com/, https://www.wired.com, http://www.independent.co.uk/, https://www.theguardian.com, http://bgr.com/, http://www.haaretz.com/, http://www.darkreading.com/, http://krebsonsecurity.com/, http://www.csoonline.com/, http://www.theregister.co.uk/, https://securityledger.com

https://www.techrepublic.com/article/infographic-charts-history-and-potential-risks-of-the-industrial-internet-of-things/

Understanding how a modern connected world changes the future of industries

- Robotics extend beyond traditional tasks of assembling and disassembling parts to a more nuanced cognitive functions with computing approaches such as Machine Learning and Artificial Intelligence
- Automation will replace certain types of roles, refine many processes, and reduce inefficiency thereby leading to better outcomes for owners of capital
- Connected electromechanical components will drive businesses forward by collecting and relaying descriptive, diagnostic, and predictive analytics in real-time
- Opportunities to interact in real-time and keeping pace with the changing market demands now become less costly due to this interconnectedness.

Understanding how a modern connected world changes the future of industries

- Manufacturers, Corporations, and institutions that produce goods will now find themselves interconnected to the vast network within their own organizations and beyond, with other suppliers, vendors, and manufacturers
- Impact from lack of raw materials or inputs into next stages of production are minimized due to efficient continuous data sharing through predictive analytics
- The need to interconnect brings in new players into the field of vendors and suppliers of components and services for e.g., new types of software programs will be required to ensure advanced robots can communicate to an industrial sensor or manage an actuator
- New IT software and hardware leads to several known and unknown vulnerabilities to surface in previously physically safe industrial processes

Industry 4.0 Threats and Opportunities

- Given the tight coupling with computing and networking systems, it also suffers from susceptibility to several new and radical forms of threats not previously anticipated when these systems were initially invented between 18th-20th centuries.

- These threats are applicable to various components within the entire environment and the impact of an industrial system breaking down could potentially threaten civilian lives in a widespread disaster – for example breakdown of an actuator at a wastewater treatment plant could pollute an entire ecosystem of water bodies in an area

- It is therefore crucial to conduct a thorough risk analysis of the environment in question so that appropriate resilience systems could be built in

enisa

Baseline Security Recommendations for IoT
in the context of Critical Information Infrastructures
November 2017

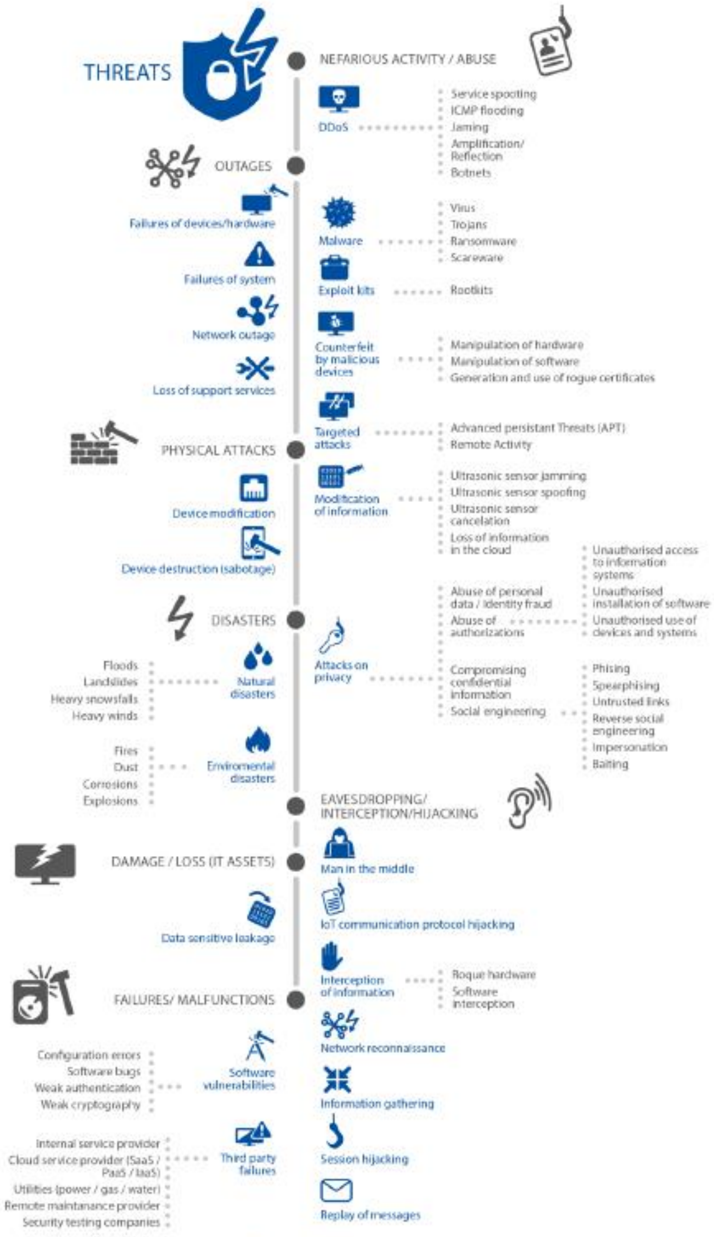
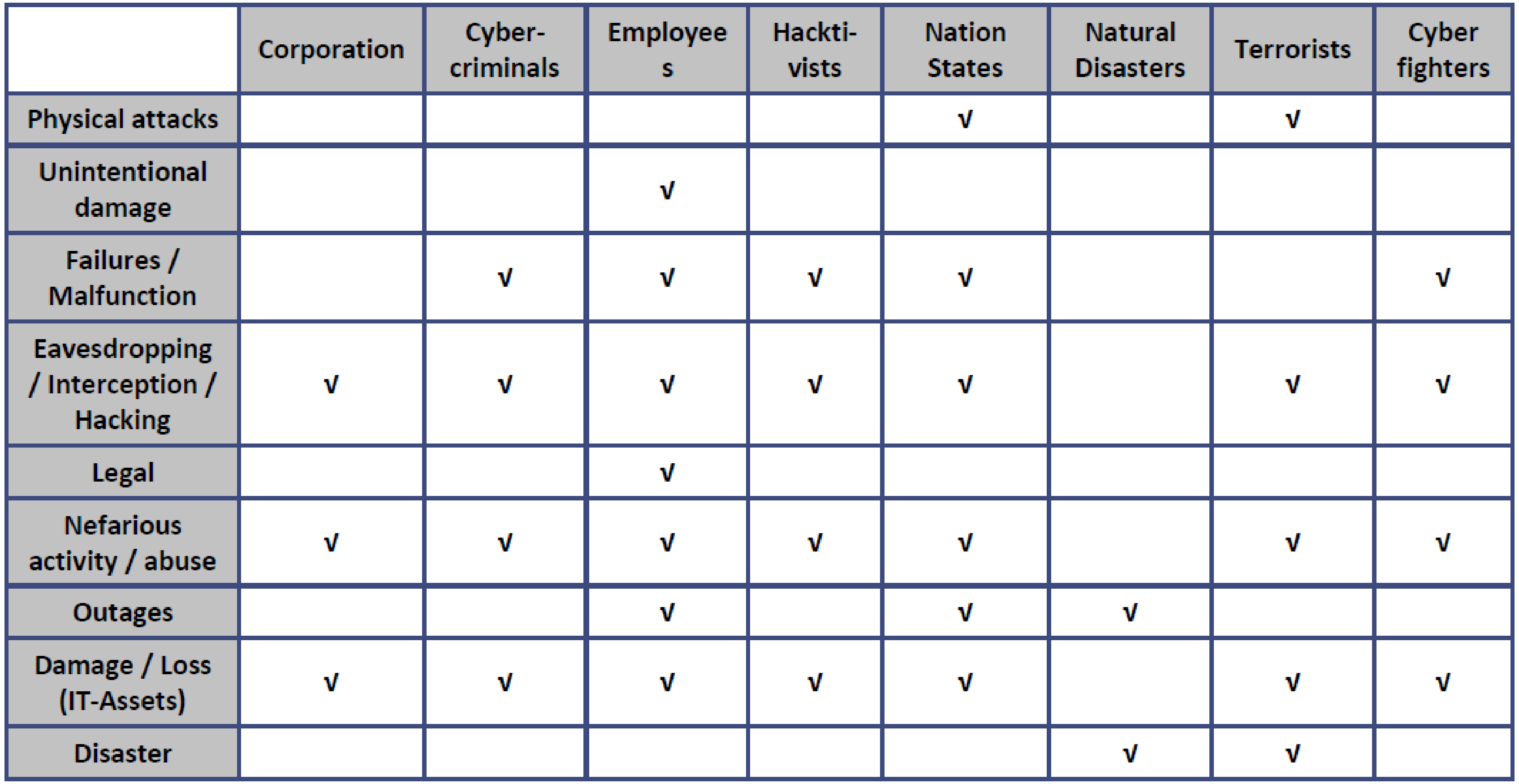

THREATS
NEFARIOUS ACTIVITY / ABUSE
DDoS
Service spoofing
ICMP flooding
Jaming
Amplification/ Reflection
Botnets
OUTAGES
Failures of devices/hardware
Failures of system
Network outage
Loss of support services
Malware
Virus
Trojans
Ransomware
Scareware
Exploit kits
Rootkits
Counterfeit by malicious devices
Manipulation of hardware
Manipulation of software
Generation and use of rogue certificates
Targeted attacks
Advanced persistant Threats (APT)
Remote Activity
PHYSICAL ATTACKS
Device modification
Device destruction (sabotage)
Modification of information
Ultrasonic sensor jamming
Ultrasonic sensor spoofing
Ultrasonic sensor cancelation
Loss of information in the cloud
Abuse of personal data / Identity fraud
Abuse of authorizations
Unauthorised access to information systems
Unauthorised installation of software
Unauthorised use of devices and systems
DISASTERS
Natural disasters
Floods
Landslides
Heavy snowfalls
Heavy winds
Environmental disasters
Fires
Dust
Corrosions
Explosions
Attacks on privacy
Compromising confidential information
Social engineering
Phising
Spearphising
Untrusted links
Reverse social engineering
Impersonation
Baiting
EAVESDROPPING/ INTERCEPTION/HIJACKING
DAMAGE / LOSS (IT ASSETS)
Data sensitive leakage
Man in the middle
IoT communication protocol hijacking
Interception of information
Roque hardware
Software interception
FAILURES/ MALFUNCTIONS
Software vulnerabilities
Configuration errors
Software bugs
Weak authentication
Weak cryptography
Third party failures
Internal service provider
Cloud service provider (SaaS / PaaS / IaaS)
Utilities (power / gas / water)
Remote maintanance provider
Security testing companies
Network reconnaissance
Information gathering
Session hijacking
Replay of messages

Figure 8: IoT Threat taxonomy

Smart Grid Threat Landscape



	Corporation	Cyber-criminals	Employees	Hacktivists	Nation States	Natural Disasters	Terrorists	Cyber fighters
Physical attacks					√		√	
Unintentional damage			√					
Failures / Malfunction		√	√	√	√			√
Eavesdropping / Interception / Hacking	√	√	√	√	√		√	√
Legal			√					
Nefarious activity / abuse	√	√	√	√	√		√	√
Outages			√		√	√		
Damage / Loss (IT-Assets)	√	√	√	√	√		√	√
Disaster						√	√	

Table 3: Involvement of Threat Agents in the threats

https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide