CYBER ACADEMY

9th International Energy Conference

Energy and Cyber Security-Risks and Protections

The risk analyses – base for the assessment of the vulnerability to cyber attacks of network information systems

Stanimir Penelov

Microsoft Certified Trainer (MCT)

mail: penelov@cyber-acad.eu
penelov@cyber-services.eu
+359 88 665 60 60

Cyber Services
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

CYBER ACADEMY

Content

CYBER ACADEMY

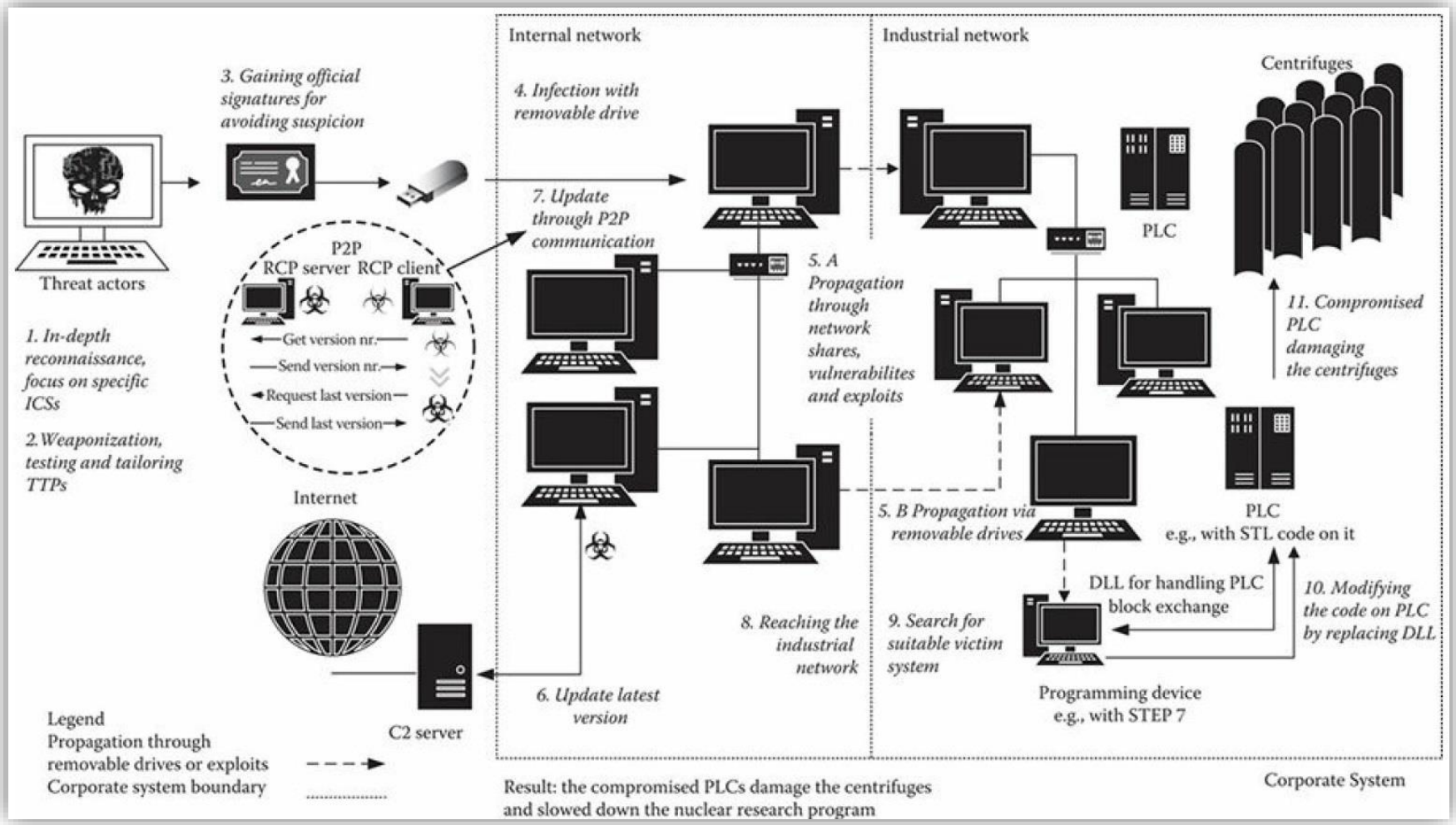
1. Examples of cyber attacks
2. Cyber Kill Chain - Lockheed Martin
3. Analysis of cyber attacks
4. Risk, Cyber risk

Content

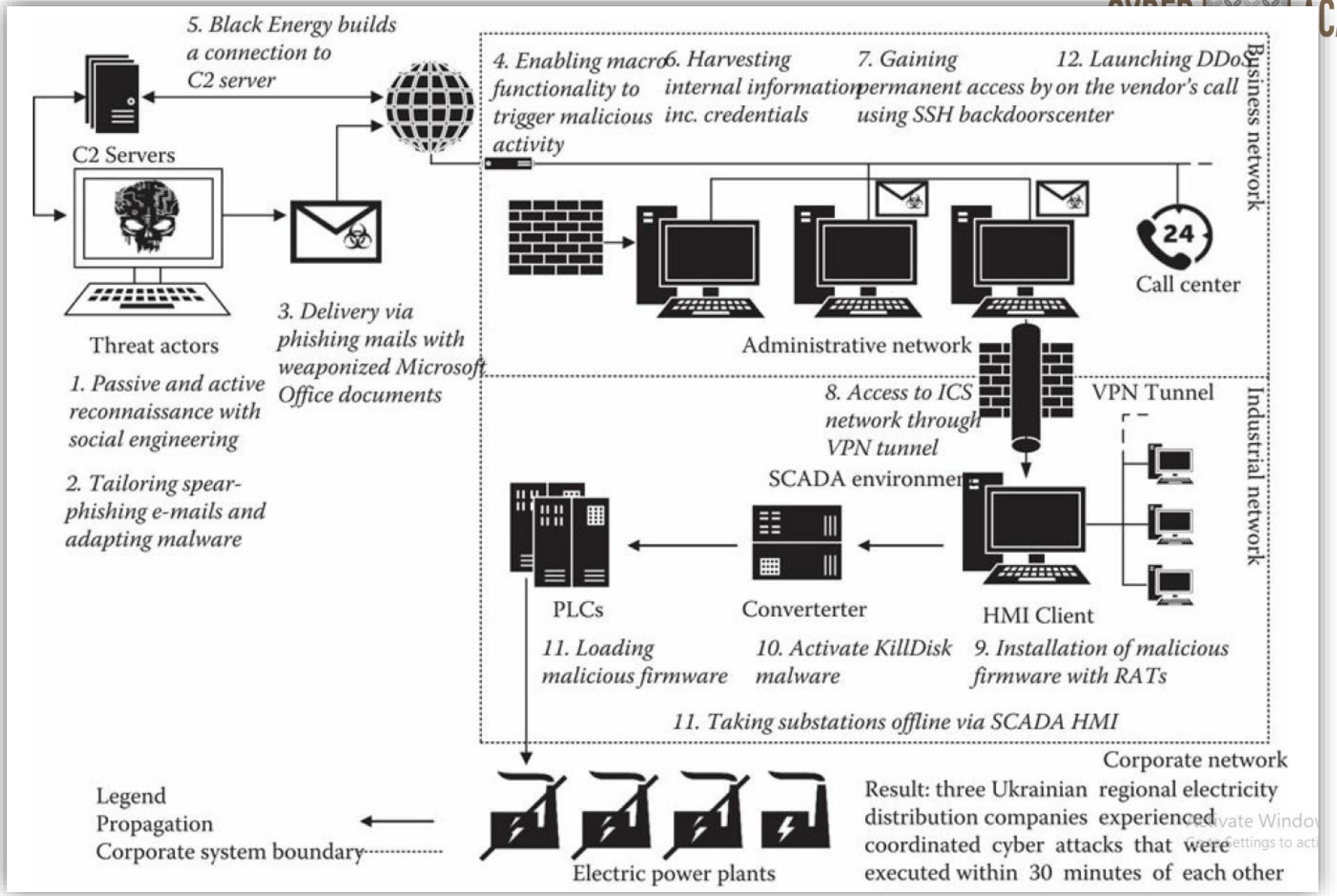
CYBER ACADEMY

1. Examples of cyber attacks
2. Cyber Kill Chain - Lockheed Martin
3. Analysis of cyber attacks
4. Risk, Cyber risk

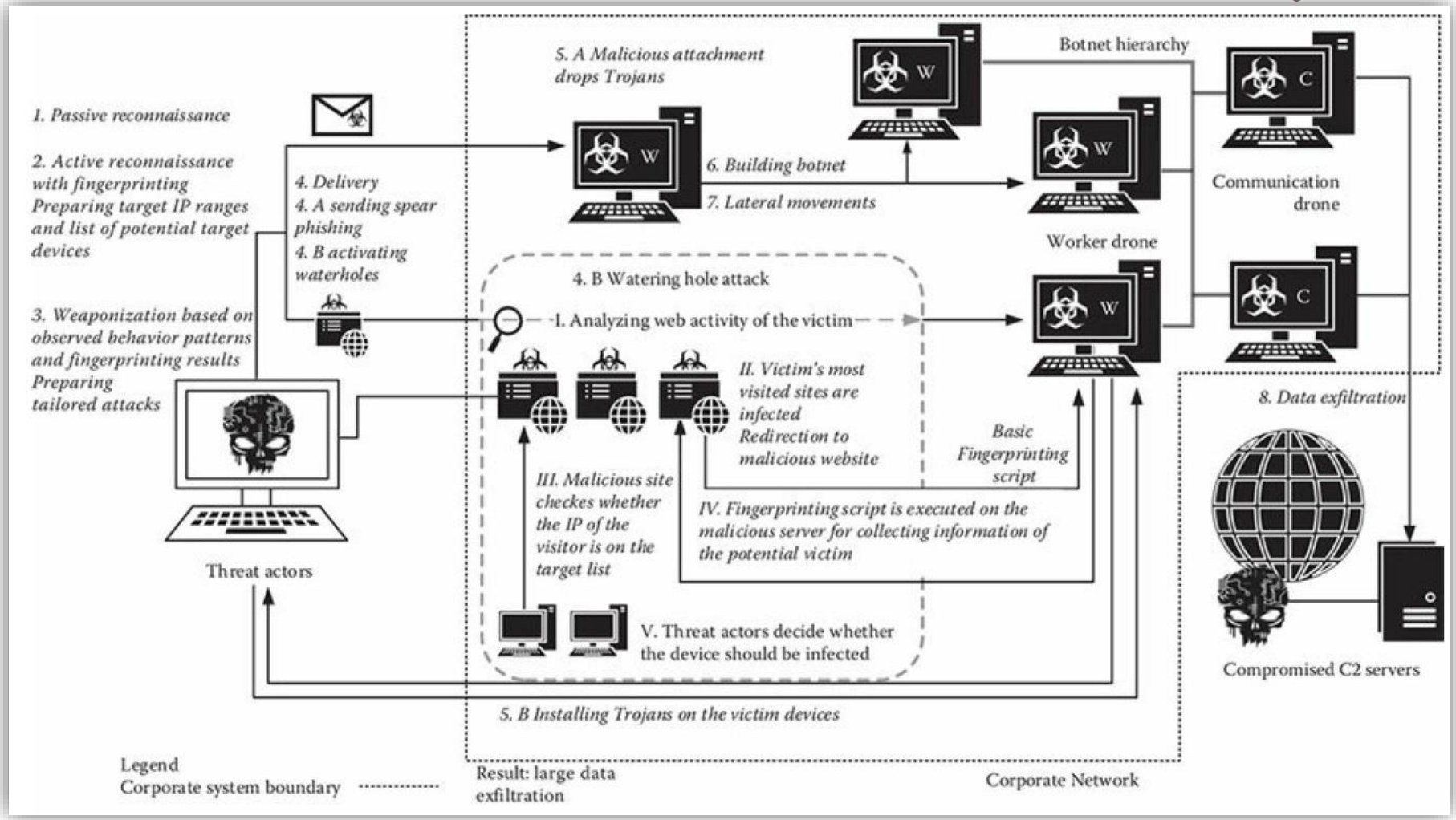
Stuxnet (2010)



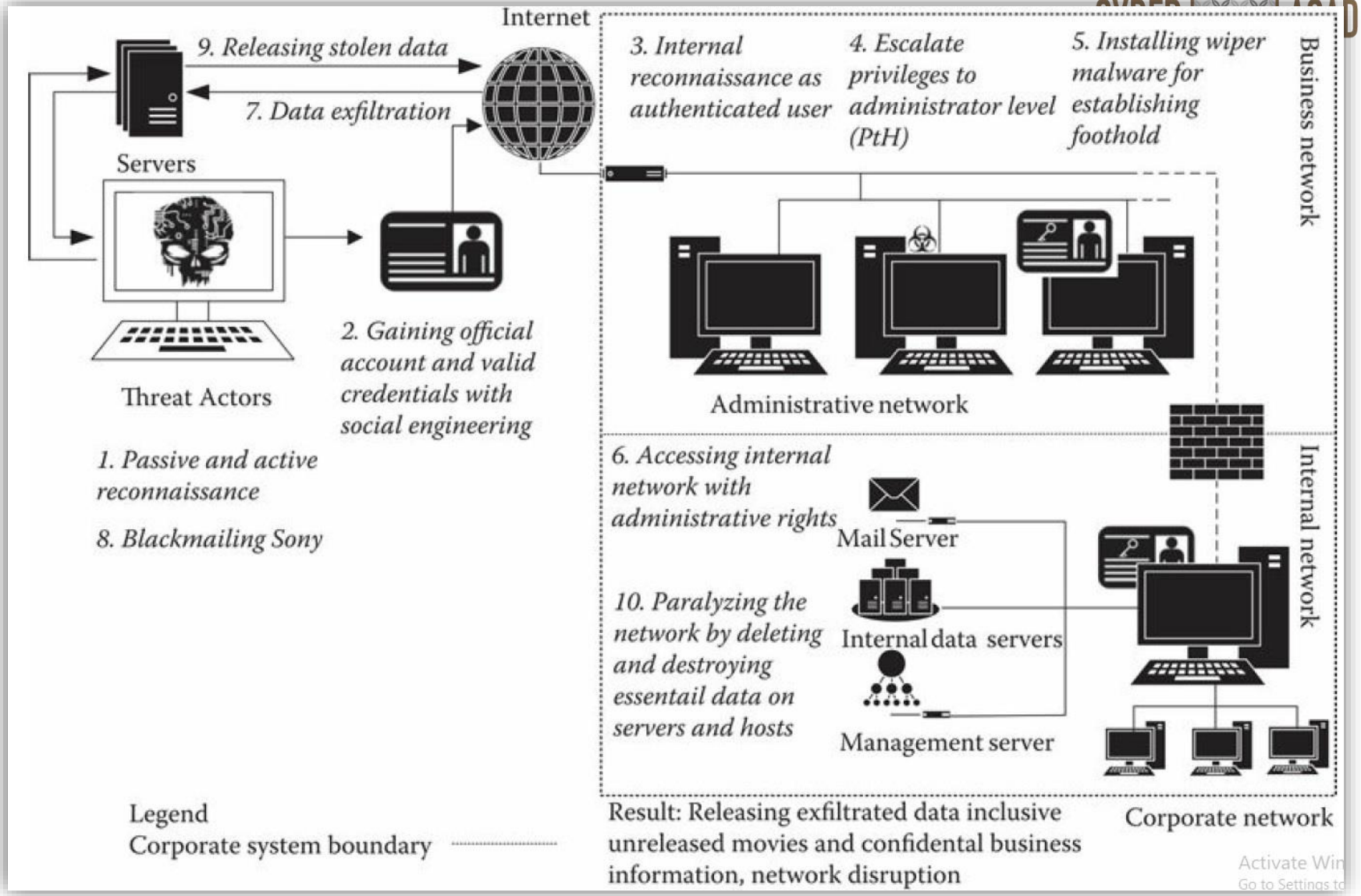
Attack illustration of the power outage in Ukraine (2015)



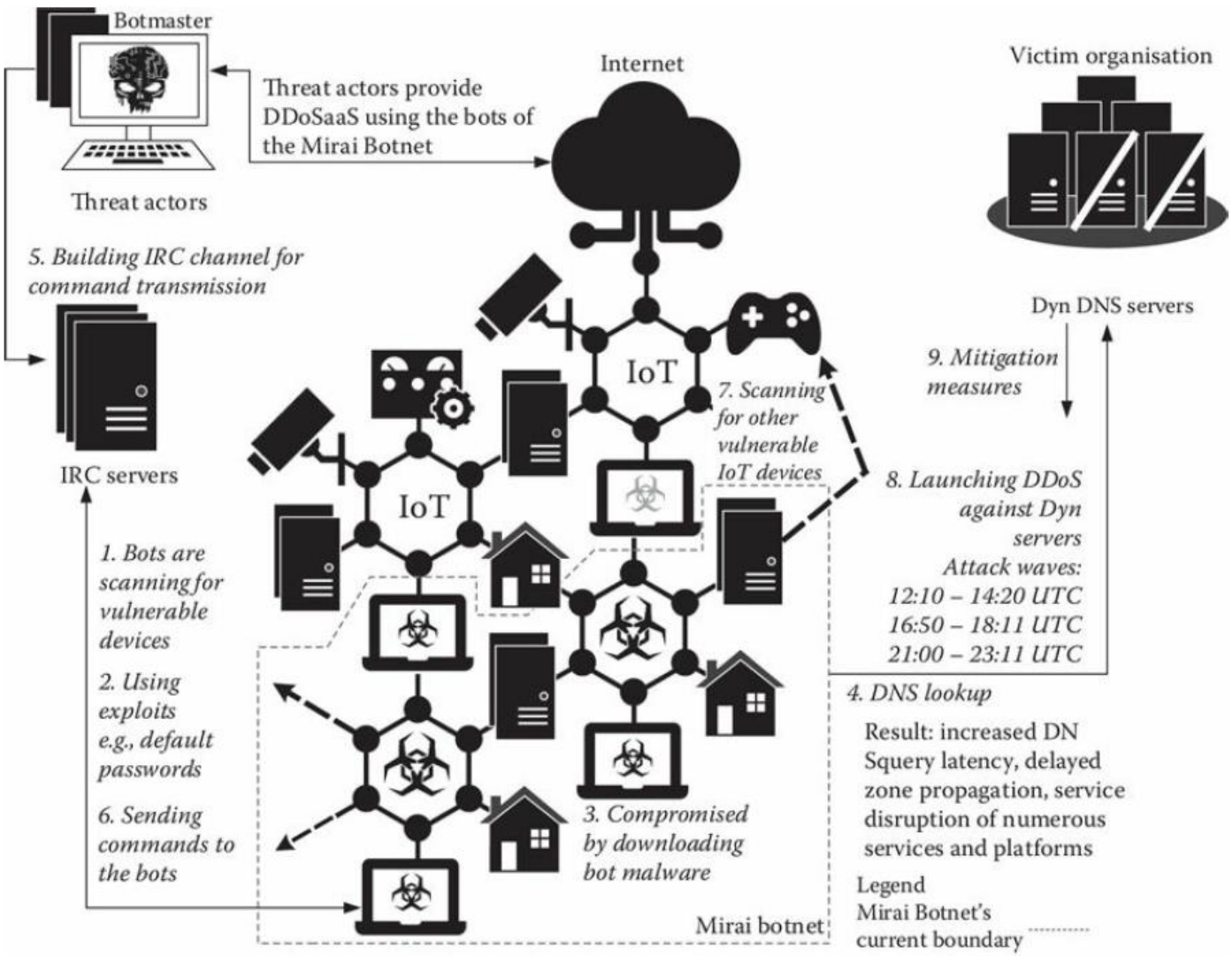
Attack illustration of the RUAG cyber espionage case (2016)



Sony Hack (2014)



Attack illustration of the IoT DDoS attack



Content

CYBER ACADEMY

1. Examples of cyber attacks
2. Cyber Kill Chain - Lockheed Martin
3. Analysis of cyber attacks
4. Risk, Cyber risk

Attack Phases

1. Identify Vulnerabilities
2. Get and Maintain Access
3. Take Advantage

Synthesis of Steps and Phases

STEPS \ PHASES	Planning	Preparation	Intrusion	Management and enablement	Sustain, entrench, develop and execute attack
Identify vulnerabilites	Reconnaissance, scanning, and enumeration (to gain useful information about the target and its weaknesses)	Analyzing and prioritizing targets; payload development; weapons pairing; acquiring (e.g., stealing) credentials			
Get and maintain access			Exploit vulnerabilities; deliver payload; use stolen credentials	Install remote access (e.g., VPNs) and other backdoors; escalate privileges and move laterally	
Take advantage				Establish command control channels; update payload as needed	Take action (exfiltrate data; move laterally; install RATs, backdoors, Clearing traces of the attack

Cyber Kill Chain - Lockheed Martin

Content

CYBER ACADEMY

1. Examples of cyber attacks
2. Cyber Kill Chain - Lockheed Martin
3. Analysis of cyber attacks
4. Risk, Cyber risk

Cyber Kill Chain - Lockheed Martin

Cyber Kill Chain	Stuxnet	Power Outage in Ukraine	Sony Hack	IOT DDoS Attack	RUAG Cyber Espionage
	☑ Passive and active reconnaissance about the specific ICS in Natanz	☑ Passive and active reconnaissance with social engineering	☑ Passive and active scanning ☑ Social engineering for gaining valid credentials	☑ Identify target ☑ Superficial reconnaissance	☑ In-depth passive and active reconnaissance ☑ Creating target IP list ☑ Fingerprinting
	☑ Professional tailoring and testing the malware ☑ In-depth preparation	☑ Tailoring spear-phishing e-mails ☑ Adapting malware	☑ Preparing wiper malware (Weaponization only after first privilege escalation)	☑ Expanding the Mirai botnet ☑ Bots are scanning for further vulnerable IoT devices	☑ Tailoring spear-phishing e-mails ☑ Preparing watering hole attacks
	☑ Delivery by infecting an external device	☑ Delivery via phishing e-mails with weaponized Microsoft Office documents	☑ Delivery via authenticated user account	☑ Delivery of malware via web-based infection or malicious attachments	☑ Delivery via spear-phishing and social-engineering or activating watering holes
	☑ Using various propagation methods partly via zero-day exploits and network shares	☑ Enabling macro functionality to trigger malicious activity	☑ Malicious activities taken as valid user ☑ Accessing the list of administrative accounts	☑ Remotely exploiting the vulnerabilities of new victims ☑ Exploit default or weak passwords	☑ Using previously prepared exploits ☑ Dropping Trojans
	☑ P2P communication between the infected devices ☑ Autonomous self-propagation	☑ BlackEnergy build connection to C2 server ☑ Gaining permanent access by using SSH backdoors	☑ Privilege escalation to admin. level ☑ AD Privilege escalation with PtH or resetting the password	☑ Transforming devices into DDoS bots ☑ Gaining shell access ☑ Deleting malicious files and traces	☑ Internal reconnaissance ☑ Creating botnet by sophisticated malware ☑ Gaining credentials and escalating privileges
	☑ Reprogramming the PLC on the ultimate targets ☑ Manipulating data displayed and deleting traces	☑ Installation of malicious firmware with RATs ☑ Activate KillDisk malware ☑ Taking substations offline ☑ Loading malicious firmware	☑ Exfiltrating data ☑ Blackmailing Sony ☑ Release stolen data ☑ Paralyzing network and releasing stolen data	☑ Launching DDoSaaS attack in several waves ☑ Causing service disruption	☑ Gaining ultimate persistence ☑ Performing PtH and PtT ☑ Gaining control over AD ☑ Stealthy data exfiltration

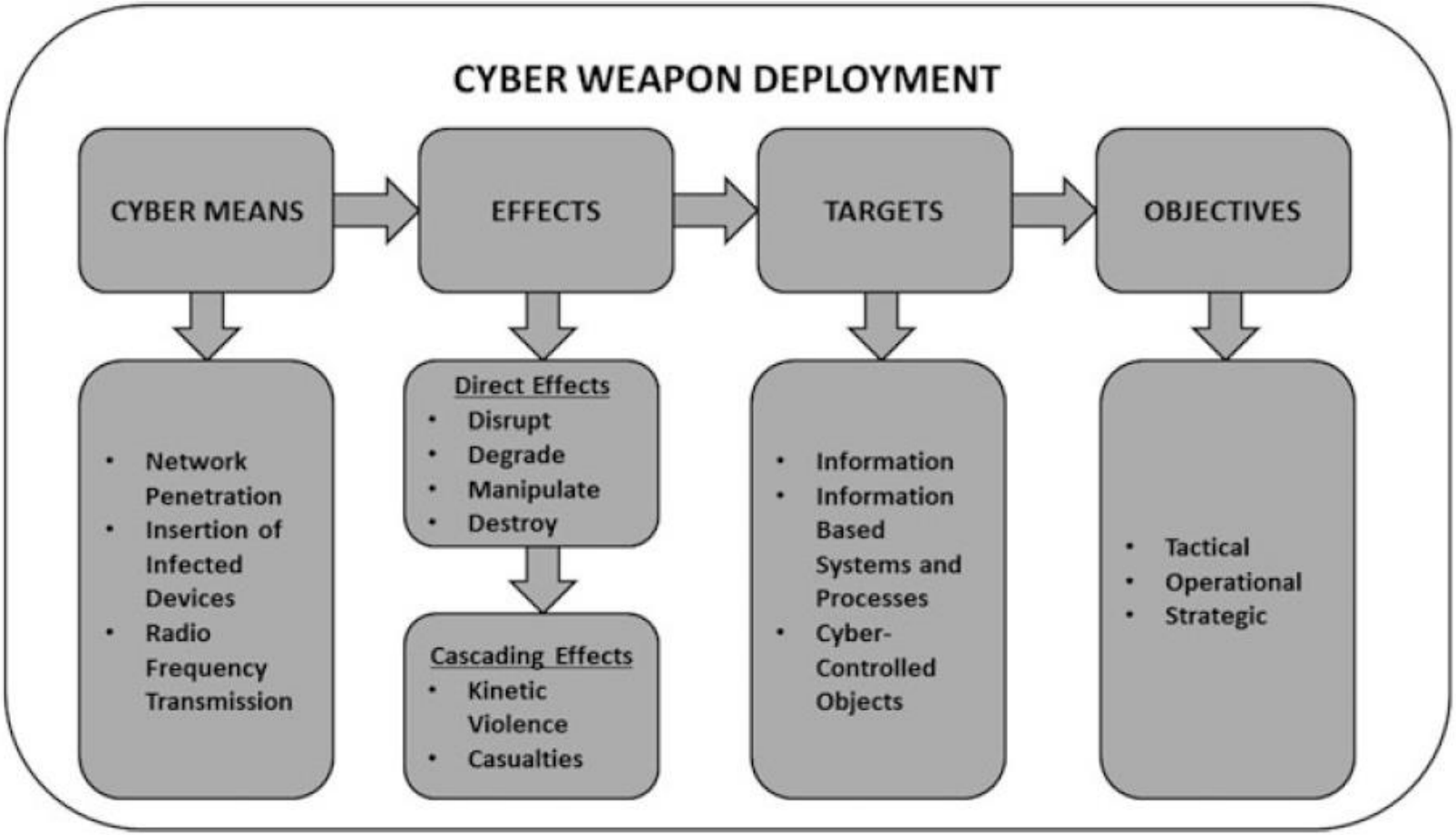
Обобщение

Attack Scenario	*Threat Actors*	*Attack Complexity*	*Aim*
Stuxnet	Nation-state-sponsored professionals	High	Sabotage
Power outage	Nation-state-sponsored professionals	High	Sabotage and espionage
Sony hack	Hacktivist	Medium	Sabotage and theft of IP
IOT DDoS attack	Unknown (hacktivist)	Medium	Sabotage
RUAG cyber espionage	Nation-state-sponsored professionals	High	Espionage and theft of IP

Характеристики на кибер атака

	Aim	*TTPs*	*Attack Scope*	*Time Scope*	*Attack*
Common Cyber Attacks	Mainly financial profit	Common TTPs, even COST	Wide-range, targets with no or low security awareness	Hit-and-run approach (hours to days)	Roughly prepared, Finite resources
APTs	Espionage and/or sabotage	Newest TTPs, even self-developed	Specific targets, targets with even high security awareness	Long-lasting with solid preparation (months to years)	Carefully prepared, Programs with well-planned modular architecture, significant resources

Framework One



Framework Two

CYBER ACADEMY

CYBER WEAPON DEPLOYMENT – BENEFITS VS DIS-BENEFITS

BENEFITS

- Cyber Weaponry Directly Achieves Strategic Objective(s) in a Manner Superior to Conventional Coercion
- Cyber Weaponry Directly Achieves Operational or Tactical Objectives that Contribute to Strategic Objective(s)
- Specific Deployment of Cyber Weaponry Reduces Associated Dis-Benefits

VS.

DIS-BENEFITS

Internal Constraints

- National Will & Identity
- Democratic Norms

Retaliation

- Attribution potential
- Coercive Capabilities of Target Actor

External Constraints

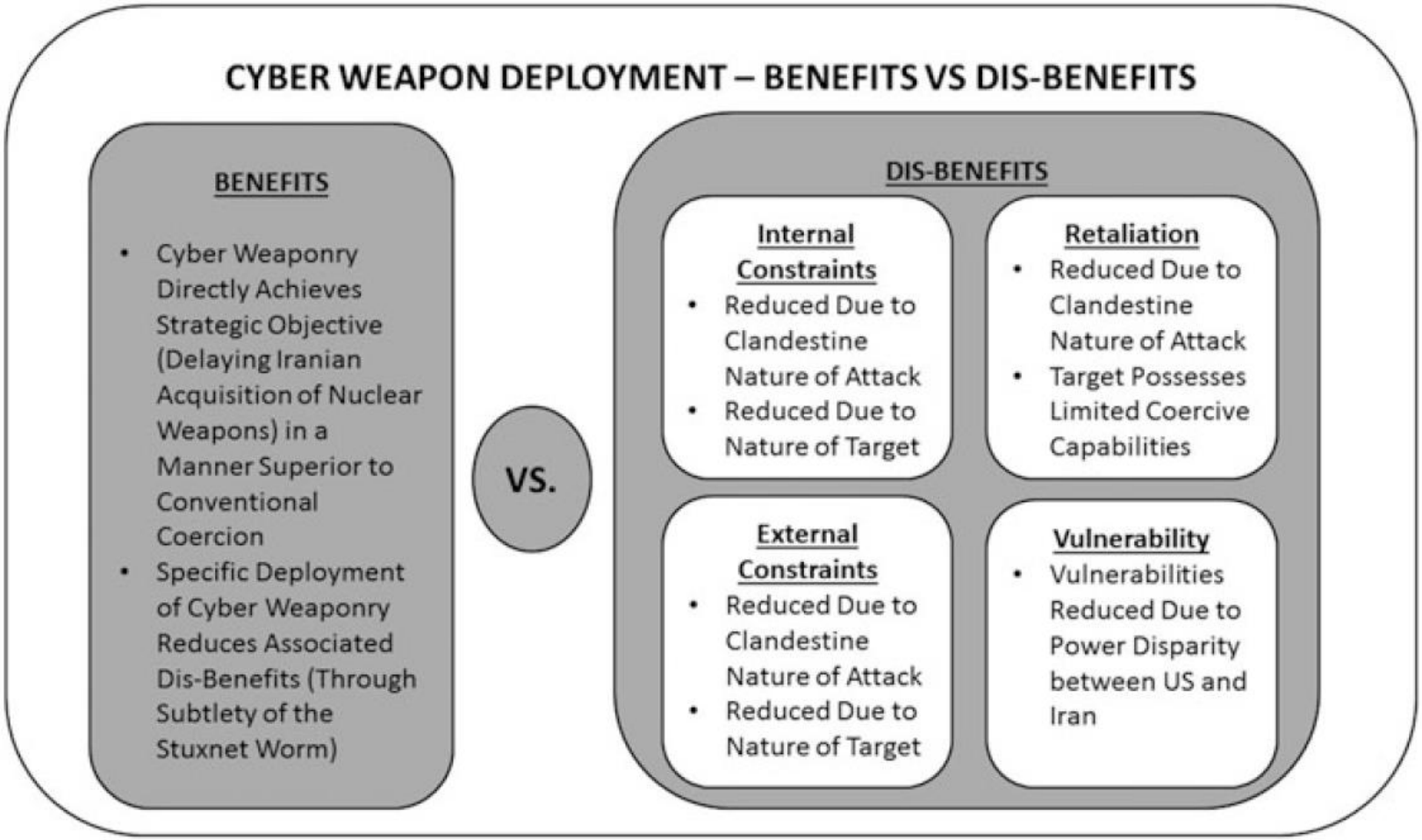
- Support from Allies
- International Condemnation/ Sanctions

Vulnerability

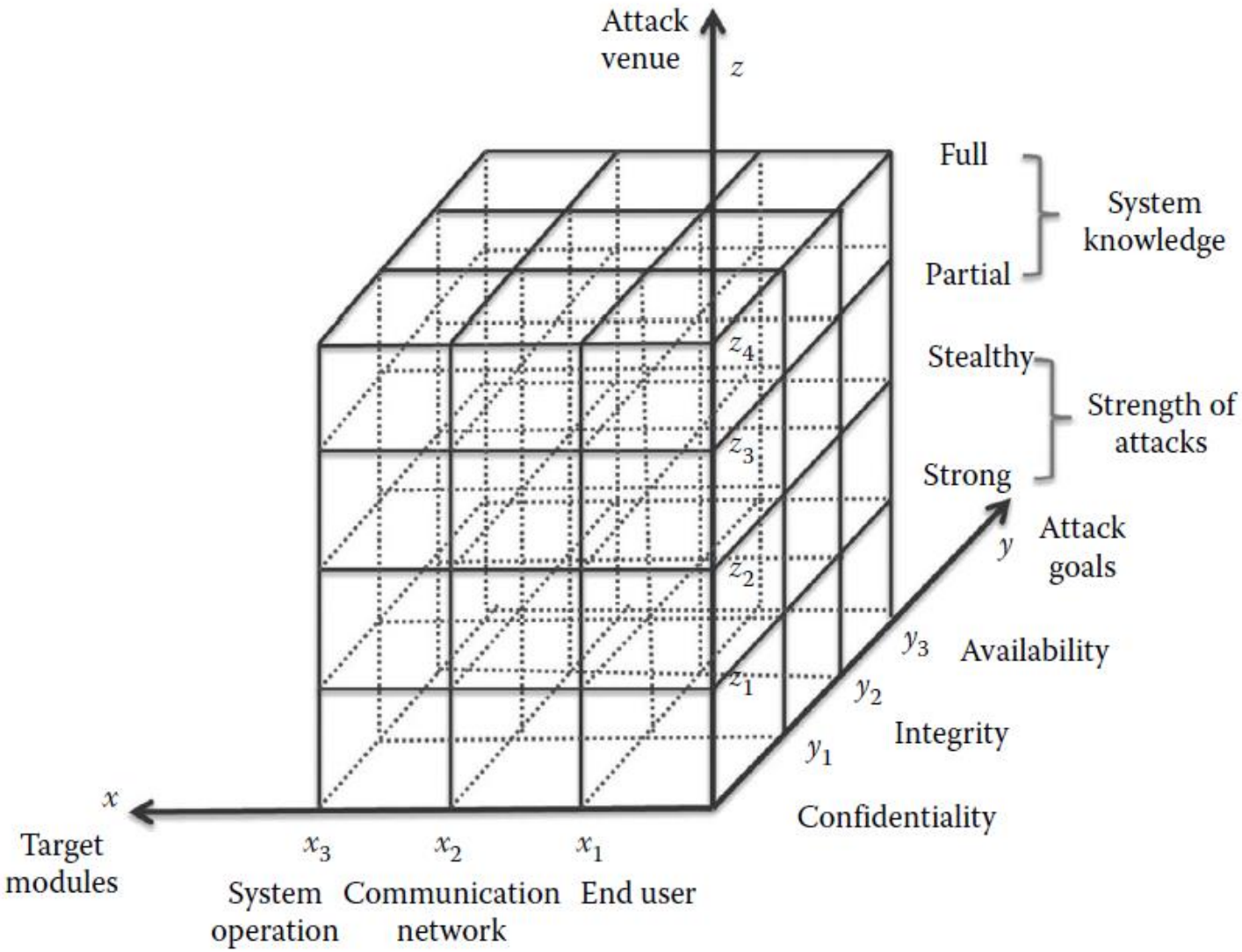
- Cyber Dependence
- Civil, Diplomatic, Economic, and Military Vulnerabilities

Анализ на Stuxnet (2010)

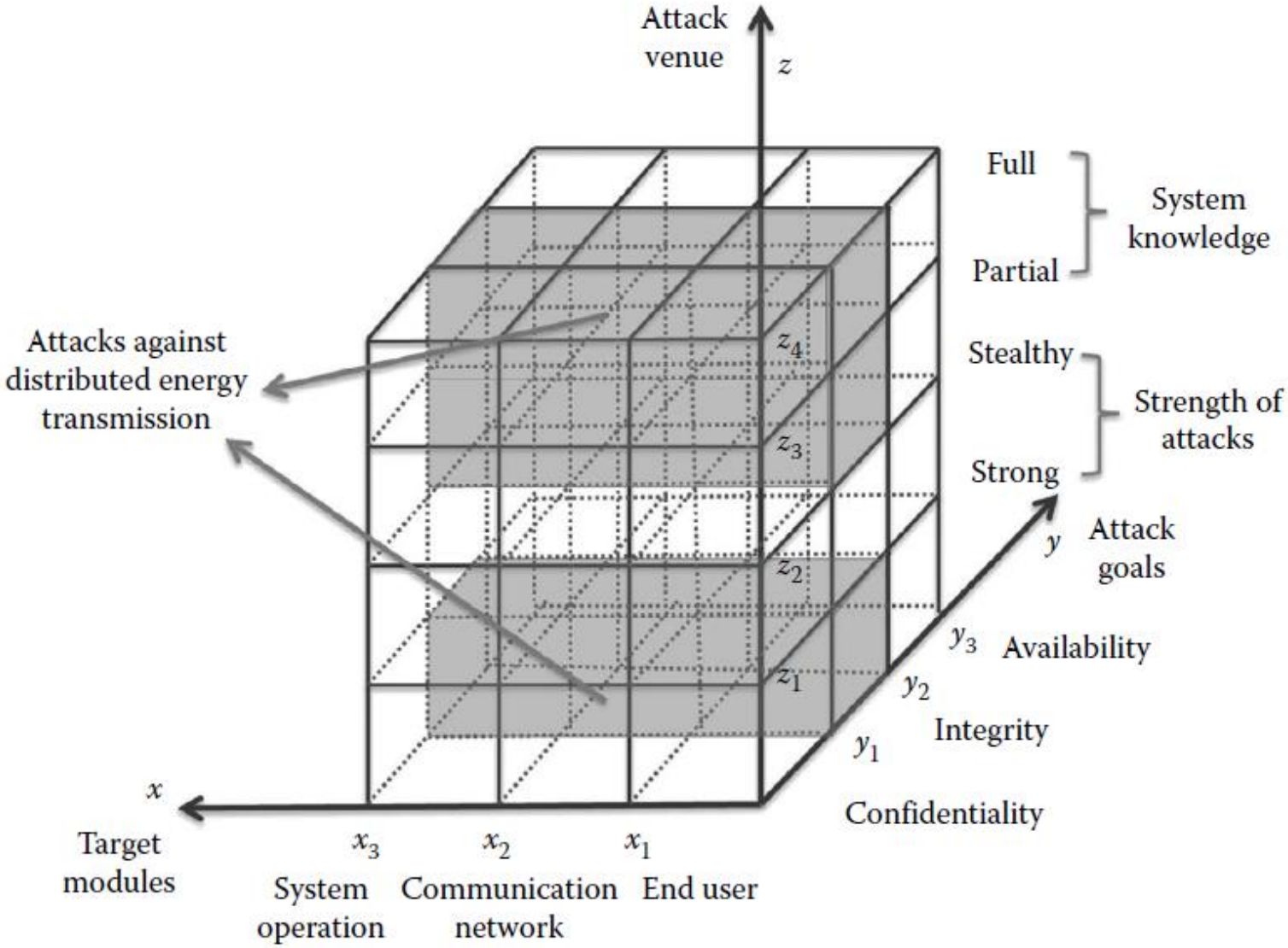
CYBER ACADEMY



3D attack space



Attacks against distributed energy transmission in 3D attack space

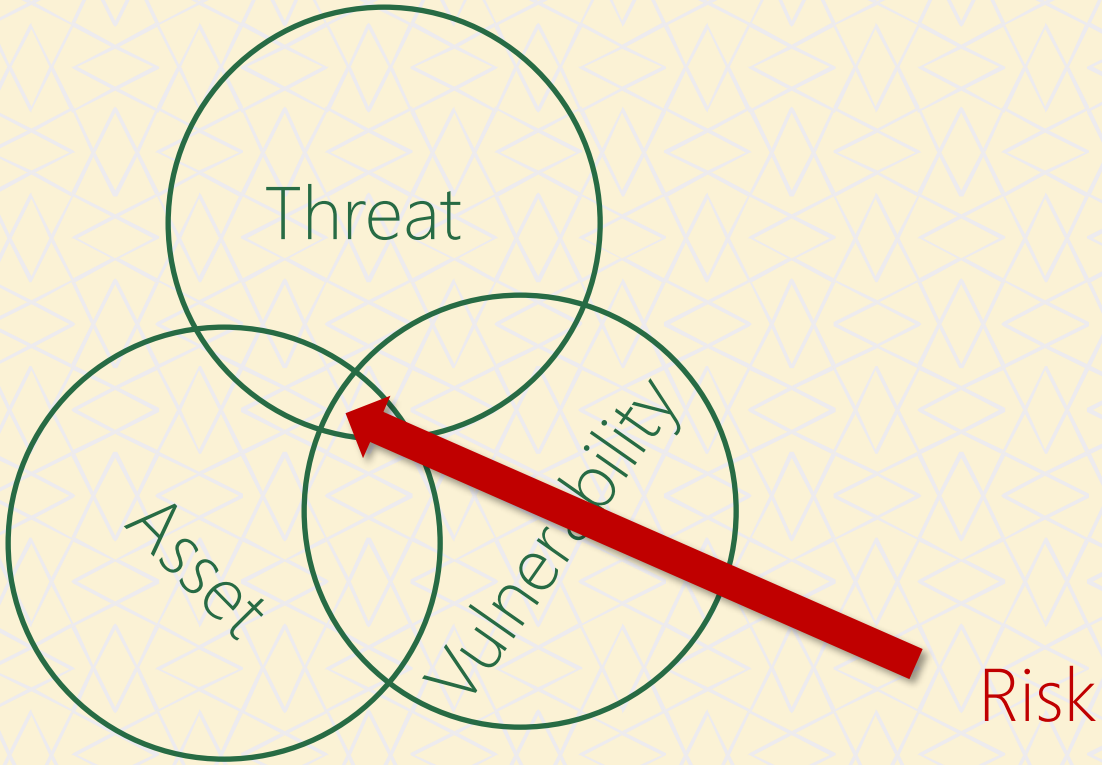


Content

CYBER ACADEMY

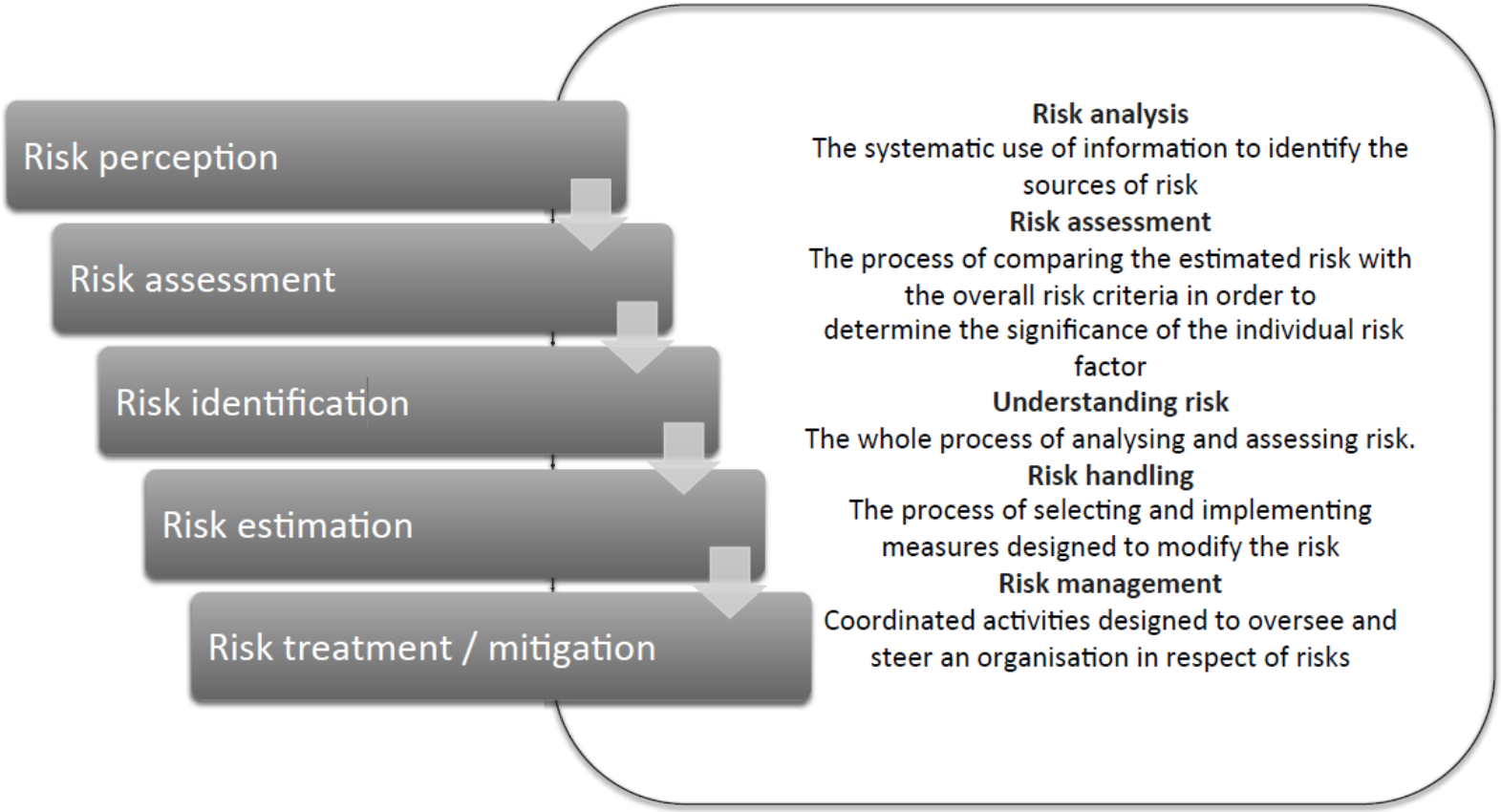
1. Examples of cyber attacks
2. Cyber Kill Chain - Lockheed Martin
3. Analysis of cyber attacks
4. Risk, Cyber risk

Risk



Управление на риска

Risk = (Vulnerability, Threat, Impact)



Кибер риск – 2 фактора

CYBER ACADEMY

CYBER RISK = $P_{Incidents}$ x LOSS PRICE

- A – Event almost never happens.
- B – Event rarely happens.
- C – The probability of an event for the considered period of time is about 0.5.
- D – Most likely, an event will occur.
- E – Event will almost certainly happen.

	Negligible	Low Risk	Low Risk	Medium Risk	Medium Risk
A	Low risk	Low risk	Low risk	Medium risk	High risk
B	Low risk	Low risk	Medium risk	Medium risk	High risk
C	Low risk	Medium risk	Medium risk	Medium risk	High risk
D	Medium risk	Medium risk	Medium risk	Medium risk	High risk
E	Medium risk	High risk	High risk	High risk	High risk

Кибер риск – 3 фактора

- $P_{incident} = P_{threat} \times P_{vulnerability}$
- CYBER RISK = $P_{threat} \times R_{vulnerabilities} \times$ LOSS PRICE

- N (Negligible) – Impact can be neglected.
- Mi (Minor) – Minor Incident: the consequences are easily removable, the costs of eliminating the consequences are not great, the impact on the information infrastructure is insignificant.
- Mo (Moderate) – An event with moderate results: eliminating the consequences is not associated with large costs, the impact on the information infrastructure is not large and does not affect the critical processes.
- S (Serious) – An incident with serious consequences: the elimination of consequences is associated with significant costs, the impact on the information infrastructure is palpable, significantly affects the critical processes.
- C (Critical) – An incident leads to an irreversible critical state and the inability to continue the business..

	Low			Moderate			High		
	Vulnerability Level			Vulnerability Level			Vulnerability Level		
SI Severity	H	C	B	H	C	B	H	C	B
Negligible	0	1	2	1	2	3	2	3	4
Minor	1	2	3	2	3	4	3	4	5
Moderate	2	3	4	3	4	5	4	5	6
Serious	3	4	5	4	5	6	5	6	7
Critical	4	5	6	5	6	7	6	7	8