Tishk International University
Faculty of Applied Science
Cybersecurity Department

Lecture 12 : Cybersecurity in Government and Military Contexts

CBS221/A : Ethics and Legal Issues in Cybersecurity

Week 13 : 28/12-01/01/2026

Instructor: Prof. Dr. Qaysar Salih Mahdi

Tishk International University

Faculty of Applied Science

Cybersecurity Department

Introduction

Cybersecurity is critical for protecting national infrastructure and military assets

Governments face threats from state and non-state actors in cyberspace

Ethical considerations are essential for cyber operations and defense strategies

https://upload.wikimedia.org/wikipedia/commons/6/63/National_cybersecurity_strategy_diagram.png

Cybersecurity in government and military contexts is crucial for national security, involving protecting critical infrastructure, sensitive data, and systems from threats like state-sponsored attacks, espionage, and cybercrime.

Key practices include threat monitoring, data encryption, advanced malware detection, and establishing network security standards, which are essential for preventing breaches and ensuring the integrity of military operations and government functions. The scope is expanding beyond traditional IT to include a wide range of interconnected systems, such as weapons, space, and mobile devices.

CYBER DEFENCE

Cyberspace is understood as the fifth domain of warfare equally critical to military operations as land, sea, air, and space. Cyber Defence (CD) is a computer network defence mechanism which includes response to actions, critical infrastructure protection and information assurance for organizations, government entities and other possible networks. CD focuses on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with.

With regard to significant socio-technological development, the forms and methods of defence are changing. Not only have armed conflicts over the last ten years clearly shown a considerable rise in the asymmetric (hybrid) nature of conflicts´ conduct, but they have also demonstrated that the use of cyberspace is of essential importance. Cyber-attacks may come unexpectedly from almost anywhere in the World. For these reasons, the cyberspace was at the NATO Summit held in Warsaw in July 2016 recognized as the fifth domain of operations in which NATO must defend itself and deter adversaries effectively.

The Czech Republic has reflected the need to curb cyber threats effectively in its National Cyber Security Strategy for the 2015 – 2020 period. The strategy clearly articulates the task to build and sustain CD capabilities. In the Action Plan, which is integral part of this strategy, Military Intelligence has been given the responsibility for the provision of CD which is being developed by the National Cyber Operations Centre for this purpose. Its task is to create an effective CD system where the Czech Republic is able to prevent, stop, mitigate and avert cyber-attacks and thus protect the population and critical infrastructure.

The Czech Government´s understanding is that CD is an autonomous specific part of a much wider concept of cyber security (CS). In this context, CD is also understood as integral part of the national defence of the Czech Republic. By the law, the defence of the Czech Republic is basically articulated as necessary measures to ensure its sovereignty and territorial integrity against external threat. Czech defence is built within given specifics of a membership in the collective defence system (NATO Alliance).

Concept for CS is that the security of cyberspace is a complex of measures to ensure integrity, confidentiality, and availability of information in cyberspace.

The difference between CD and CS lays most of all in the nature and the intensity of cyber-attacks and consequently, a possible response also differs. Furthermore, it is not always possible to ascertain whether CD or CS should be applied. Therefore, being prepared against cyber-attacks means to build a complex and holistic system that is continual in the time being. It is not enough to concentrate only on security domain of cyberspace. We need to be ready to face attacks that will have the potential to activate the defence of the state. Only the most intensive and massive cyber-attacks will activate full mighty of CD. Conceptually, CD is defined as integral part of much wider measures on state level to defend the Czech Republic during extraordinary situations.

Why Military Intelligence?

First of all, Army of the Czech Republic is responsible for defence and the Military Intelligence is an integral part of the Ministry of Defence (MoD). Being an integral part of MoD means both better coordination with the Army and continuity of taken measures on defence during crises. Moreover, there is the relevant fact that Military Intelligence is the only intelligence service in the Czech Republic that has both external and internal competencies.

In addition, cyberspace is not a common battlefield, it is more about information space where intelligence services traditionally play an important role. In the majority of attacks, it is not possible to attribute them convincingly. A nature of cyber-attack might hold terroristic, criminal, espionage or many other aspects. Therefore, it is complex, complicated, if not tricky to decide whether it is correct to activate full (partial) self-defense measures on state level or not.

Tishk International University
Faculty of Applied Science
Cybersecurity Department

National Security and Cybersecurity

National Security and Cybersecurity

Protecting critical infrastructure, communications, and government networks

Risk Assessment Equation: $R = T \times V \times I$ (R=Risk, T=Threat, V=Vulnerability, I=Impact)

Practical Example: $T=0.7$, $V=0.5$, $I=0.9$ → $R=0.315$ → High risk

Exercise: $T=0.4$, $V=0.6$, $I=0.8$ → Compute R and classify risk

Solution: $R = 0.4 \times 0.6 \times 0.8 = 0.192$ → Medium risk

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Cyberwarfare

Cyberwarfare

Cyberwarfare: Digital attacks by nations to disrupt adversary systems

Attack Probability: P_a = 1 - e^(-λ t) (P_a = probability, λ = attack rate, t = time)

Practical Example: λ=0.1/day, t=7 → P_a ≈ 0.503 (~50%)

Exercise: λ=0.05/day, t=10 → compute P_a

Solution: P_a = 1 - e^-0.5 ≈ 0.393 (~39%)

https://upload.wikimedia.org/wikipedia/commons/4/47/Cyberwarfare_attack_diagram.png

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Ethical Implications

Ethical Implications

Balancing surveillance and civil liberties

Offensive cyber operations and international law

Responsibility for collateral damage

Practical Example: Monitor citizens ethically → minimal data collection, transparency, legal compliance

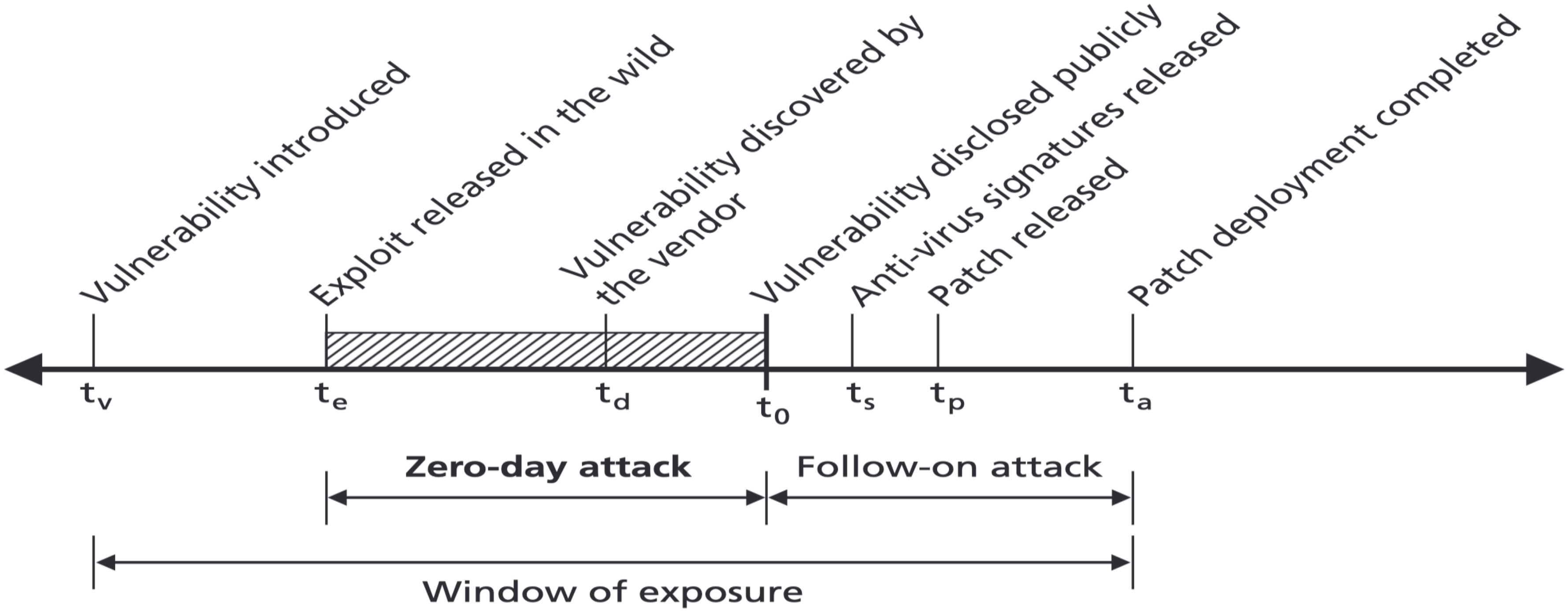
Exercise: Implement surveillance on 10,000 citizens ethically → propose safeguards

Solution: Data anonymization, access control, oversight committee, retention policies

https://upload.wikimedia.org/wikipedia/commons/3/3f/Cyber_ethics_framework_diagram.png

Tishk International University
Faculty of Applied Science
Cybersecurity Department

Case Studies
Cyberattack time line


Vulnerability introduced
Exploit released in the wild
Vulnerability discovered by the vendor
Vulnerability disclosed publicly
Anti-virus signatures released
Patch released
Patch deployment completed
t_v
t_e
t_d
t_0
t_s
t_p
t_a
Zero-day attack
Follow-on attack
Window of exposure

Case Studies

Stuxnet (2010): Cyber sabotage of Iran’s nuclear facilities → Mitigation: patch systems, network segmentation, employee training

Estonia Cyberattack (2007): DDoS attack → Mitigation: redundant servers, traffic filtering, ISP collaboration

NotPetya (2017): Global malware → Mitigation: backups, awareness, threat intelligence

https://upload.wikimedia.org/wikipedia/commons/0/0b/Cyberattack_timeline_diagram.png

Conclusion

Cybersecurity is crucial for national security and military defense

Cyberwarfare presents operational and ethical challenges

Continuous risk assessment, training, legal frameworks, and ethical oversight are essential

References

Clarke, R., & Knake, R. (2010). Cyber War: The Next Threat to National Security

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know

Thank you for your listening