Russian Threats & Cyber Operations

Oleksii Baranovskyi, Ph.D., CISSP, CISM, CEH, etc.

Based on real cases and history

I am Ukrainian. We have fighted. We are fighting. We will win.

Timeline of detected attributed cyber operations

1999 - Moonlight Maze investigation concludes that the first ever massive data breach of classified Pentagon and NASA documents was traced back to an IP in Moscow. In testimony before Congress, James Adams, CEO of Infrastructure Defense Inc, stated that, "the value of this stolen information is in the tens of millions, perhaps hundreds of millions of dollars."

2007 - After the Estonian government removed a Soviet war monument from downtown Tallinn, Russia-based attackers launch a series of denial of service attacks against Estonian public and private sector organizations. This is the first time that a foreign actor threatened another nation's security and political independence through primarily cyber operations.

2008 - Two weeks before Russia's invasion of Georgia, Russia-based attackers launch distributed denial of service (DDOS) to swamp and disable Georgian government websites.

2014 - Prior to the Ukrainian presidential elections, Russian hackers affiliated with the GRU's Main Intelligence Directorate carry out a series of cyberattacks to manipulate the vote. The CyberBerkut hackers invaded the network and deleted files in an attempt to change the election results by targeting Kyiv's Central Election Commission.

Timeline of detected attributed cyber operations

2015 - Cyberattack (BlackEnergy) to “Prykarpatya oblenergo”, first attack caused power outage, western Ukraine.

2016 - The FBI opens the “Crossfire Hurricane Investigation” amid increasing evidence and public discourse about Russian interference in the 2016 U.S. presidential elections through cyberespionage and information operations. The Russian intelligence community enters a period of internal turbulence as individual departments avoid responsibility for blowing cover.

2016 - The interference in the US election and the resulting backlash from the US intelligence community provoked a big internal crisis in Moscow where officials blamed each other for getting caught. The FSB’s Information Security Center, in charge of counterintelligence, is decimated by internal purges.

2016 - Cyberattack (Indestroyer) to “Kyiv oblenergo”, second attack caused power outage, the central Ukraine, capital.

2016 - Series of cyberattacks to governmental entities in Ukraine (Ukrzaliznytsya, Ministry of Infrastructure, etc.)

Timeline of detected attributed cyber operations

2017 - A series of powerful malware attacks, known as XData, WannaCry, NotPetya, swamp the systems of Ukrainian organizations, including banks, government ministries, electricity firms, newspapers, etc.

2017 - Two days before the final vote in the French presidential election, Russian hackers leak more than 15 GB of stolen data, including 20.000 emails, from Emmanuel Macron's campaign staff.

2020 - Russian state-affiliated hackers breach the SolarWinds Orion system, resulting in one of the biggest cybersecurity breaches in 21th century. With supply chain attack hackers infiltrated several US agencies, Pentagon, Department of Homeland Security, Microsoft, Cisco, etc.

2021 - The Russia-affiliate Darkside hacking group attacks and shuts down the Colonial pipeline.

2022 - In the month leading up to Russia's invasion of Ukraine, Russia launches:

- series of DDoS attacks against banking and government websites
- supply chain attack **#attack13** with defacing the sites and publishing the **BULK DATA LEAKS FREE** (Diia, MIA, Car register, etc.)

Timeline of detected attributed cyber operations

1 hour before invasion - VIASAT hack

(destructive “wiper” malware called AcidRain against Viasat modems and routers)

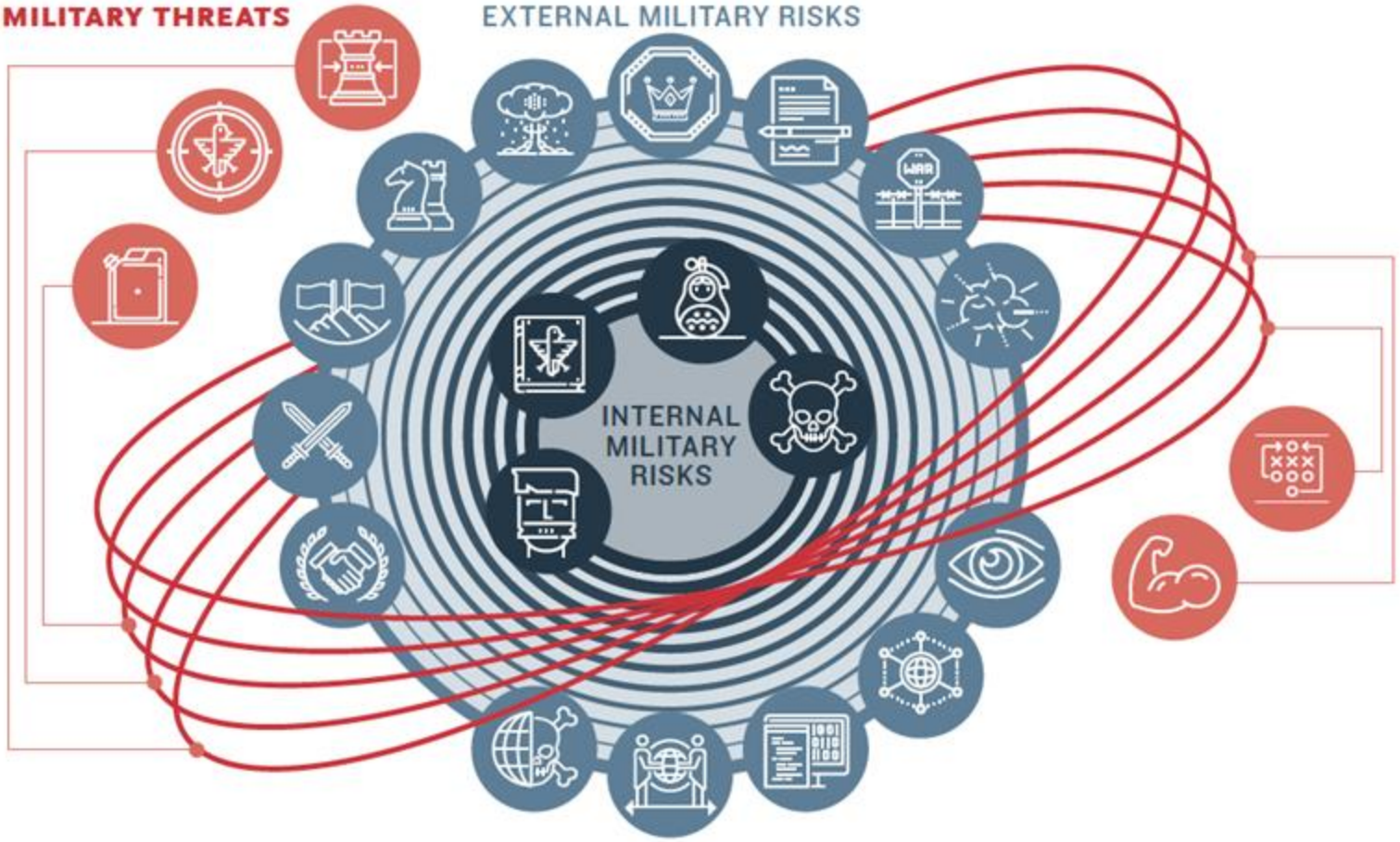
“This is what I can say about cyberattacks or war of words in the press and other issues. Action always causes reaction. Always.”

Vladimir Putin, President of the Russian Federation (2018)

Everything came from doctrine

2000 - Vladimir Putin signs the “Doctrine of the Information Security of the Russian Federation.” The list of the country’s higher education institutions which provide training in information security is expanded.

“The Military Doctrine of the Russian Federation,” Approved by the President of the Russian Federation on December 25, 2014, The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, June 29, 2015, https://rusemb.org.uk/press/2029.


MILITARY THREATS
EXTERNAL MILITARY RISKS
INTERNAL MILITARY RISKS

EXTERNAL MILITARY RISKS

- Expansion and strengthening of North Atlantic Treaty Organization (NATO)
- Global or regional destabilization
- Deployment of military forces adjacent to Russia or its allies
- Undermining of Russian strategic deterrence capabilities
- Violation of Russia's or allies' territorial integrity or sovereignty
- Proliferation of weapons of mass destruction and missile technology
- Failure to comply with international agreements and treaties
- Armed conflict adjacent to Russia or its allies
- Unauthorized use of foreign military force adjacent to Russia or its allies
- Growth of transnational non-state threats like terrorism or organized crime
- Growth of ethnic, religious, or cultural disagreements over territorial borders
- Illicit use of cyber or information operations against Russia or its allies
- Establishment of hostile states adjacent to Russia
- State-sponsored subversive activities targeting Russia

INTERNAL MILITARY RISKS

- Provocation of Russian political strife
- Separatist and ethno-religious terrorism
- Undermining of Russian historical, spiritual, and patriotic traditions
- Provocation of Russian cultural strife

MILITARY THREATS

- Sharp deterioration of interstate relations
- Disruption of key Russian military capabilities or critical sectors
- Support of armed insurrection in Russia or its allies
- Use of military force during exercises adjacent to Russia or its allies
- Heightened combat readiness

Response to the risks and threats

Identify and assess potential risks and threats
Respond to concrete risks and threats

Cyber Operation Significance

Military Engagement	Concept	CO Significance
Awareness of potential military risks and threats	The ongoing use of technical means to collect information to identify emerging military risks and threats at the regional and global level.	Cyber operations are used to conduct espionage against political and military targets.

Gemaredon/Actinum, Fancy Bear/Strontium, Callisto/Seaborgoium

Cyber Operation Significance

Military Engagement	Concept	CO Significance
Widespread use of advanced weapons and technologies	The use of a broad range of weapons that employ advanced technologies such as computerization, directed energy, robotics, and unmanned flight	Cyber operations' tools may be advanced military technologies that provide an advantage over other states that lack the technical or financial capacity to develop, acquire, or defend against them.

Cyber Operation Significance

Military Engagement	Concept	CO Significance
Warfare impacting the entire depth of an enemy's territory simultaneously	The ability to cause widespread harm to an adversary across its physical or digital battlefield.	Cyber operations should be able to cause widespread harm to a targeted country's computerized devices.

Sandworm/Iridium , Energetic Bear/Bromine

Cyber Operation Significance

Military Engagement	Concept	CO Significance
Precise destructive attacks	The ability to selectively destroy targets rather than cause indiscriminate damage.	Cyber operations should be able to cause highly targeted destruction with precise outcomes

Cyber Operation Significance

Military Engagement	Concept	CO Significance
Reduced time to launch military operations with preemptive activities	The time between the appearance of a cause for action and acting must be minimized.	Precise destructive cyber attacks normally have protracted timelines. Preemptive establishment of persistent access to high-value digital and computerized targets (“prepping the battlefield”) is thus necessary.

VIASAT case

Cyber Operation Significance

Military Engagement	Concept	CO Significance
Global computerized command and control	The use of computer systems to provide unified situational awareness, enabling unified decision among dispersed military forces. Subordinate forces can take initiative with surprise, decisiveness, and aggressiveness.	Cyber operators are empowered to take rapid, decisive action.

Cyber Operation Significance

Military Engagement	Concept	CO Significance
Creation of permanent war zones	Modern warfare creates a state of constant conflict, denying the adversary an opportunity to regroup and reassess, increasing the adversary's stress and confusion.	Cyber operations can maintain a state of constant conflict with limited risk of escalation.

Cyber Operation Significance

Military Engagement	Concept	CO Significance
Irregular and privatized warfare	The involvement of irregular or nonstate combatants in warfare, encompassing militias, terrorists, and private military companies.	Cyber operations can use hired contractors, mercenaries, or other nonstate actors to achieve military outcomes. This characteristic also includes regular military operators' use of fake nonstate personas to accomplish military objectives.

Conti group, Evil corp

Cyber Operation Significance

Military Engagement	Concept	CO Significance
Indirect and asymmetric warfare	The ability to neutralize threats without deploying a parity of forces.	Cyber operations typically need fewer forces and less material than kinetic warfare.

Cyber Operation Significance

Military Engagement	Concept	CO Significance
Manipulation of social or political environment	The attempt to influence, control, or instigate political and social movements, with the objective of either weakening the opponent socially or installing friendlier politicians.	Cyber operations can bolster political and social manipulation efforts, such as harming the reputation of political and social targets with provocative data leaks and disinformation.

Latest EU public cases

- A **company** working in the **security business** had a **breach** with malware installed in many parts of the infrastructure. The attack was performed by either an **Initial Access Broker** (IAB) or a ransomware affiliate with a **probable Russian origin** and had deployed several different types of malwares in the environment, one of them a malware publicly known only used on Windows platform that had been ported to Linux. Additionally, the command and control infrastructure used by the threat actor has also been used by the Conti ransomware gang.

- A company within **critical infrastructure** was **breached** and **data stolen**. The threat actor had deployed malware in both the **enterprise** and the **OT systems**. In this incident ransomware was never deployed but instead data was wiped. The threat actor **could be attributed** to **Russian cybercriminals** that shared command and control infrastructure with **BlackCat** ransomware gang.

- Several cases of **Raspberry Robin** have been detected and blocked in the initial execution stage in **Truesec SOC**. This was before the download of the second stage of the malware. Raspberry Robin has been attributed by Microsoft to the Russian ransomware gang **Evil Corp**.

Three Strategic Domains

Conventional

- Conflict is inevitable
- Need to prepare / be ready
- Attack/Defense evolution

Non-Conventional (Nuclear)

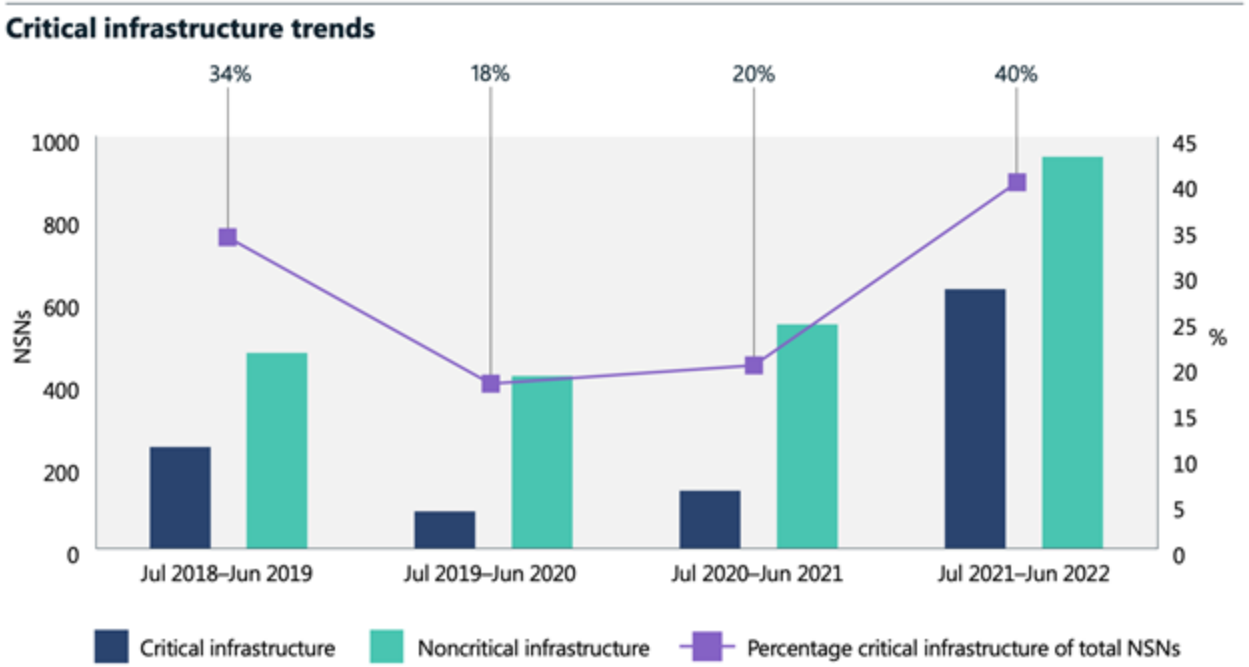
- Conflict is catastrophic
- Defense is losing
- Attack is losing 5 minutes after

Cyber

- Conflict is constant
- **Continuous fight** for the **initiative**
- Cyberconflict is alternative the war?

Cyber Persistence Theory: Redefining National Security in Cyberspace (Bridging the Gap)

Current State-of-art



- Microsoft Digital Defence Report 2022

Outside of Ukraine, Microsoft detected Russian network intrusion efforts against **128 organizations** in **42 countries** between late February and June. **The United States** was Russia's **number one target**. **Poland**, through which much of the international military and humanitarian assistance to Ukraine transits, was also a significant target during this period. Threat actors affiliated with the Russian state pursued organizations in Baltic countries and computer networks in **Denmark**, **Norway**, **Finland**, and **Sweden** in **April** and **May** as well.

Microsoft Digital Defence Report 2022

TRUESEC

Any questions?