RACI
RIPE Academic Cooperation Initiative

Hybrid nature of modern threats for cybersecurity and information security

by
Oleksandr Tsaruk and Maria Korniiets

"The more we think about how to harness the technology revolution, the more we will examine ourselves and the underlying social models that these technologies embody and enable, and the more we will have ***an opportunity to shape the revolution*** in a manner that improves the state of the world."

— Klaus Schwab (2017), The Fourth Industrial Revolution

Two limiting factors that may constrain of Industry 4.0.

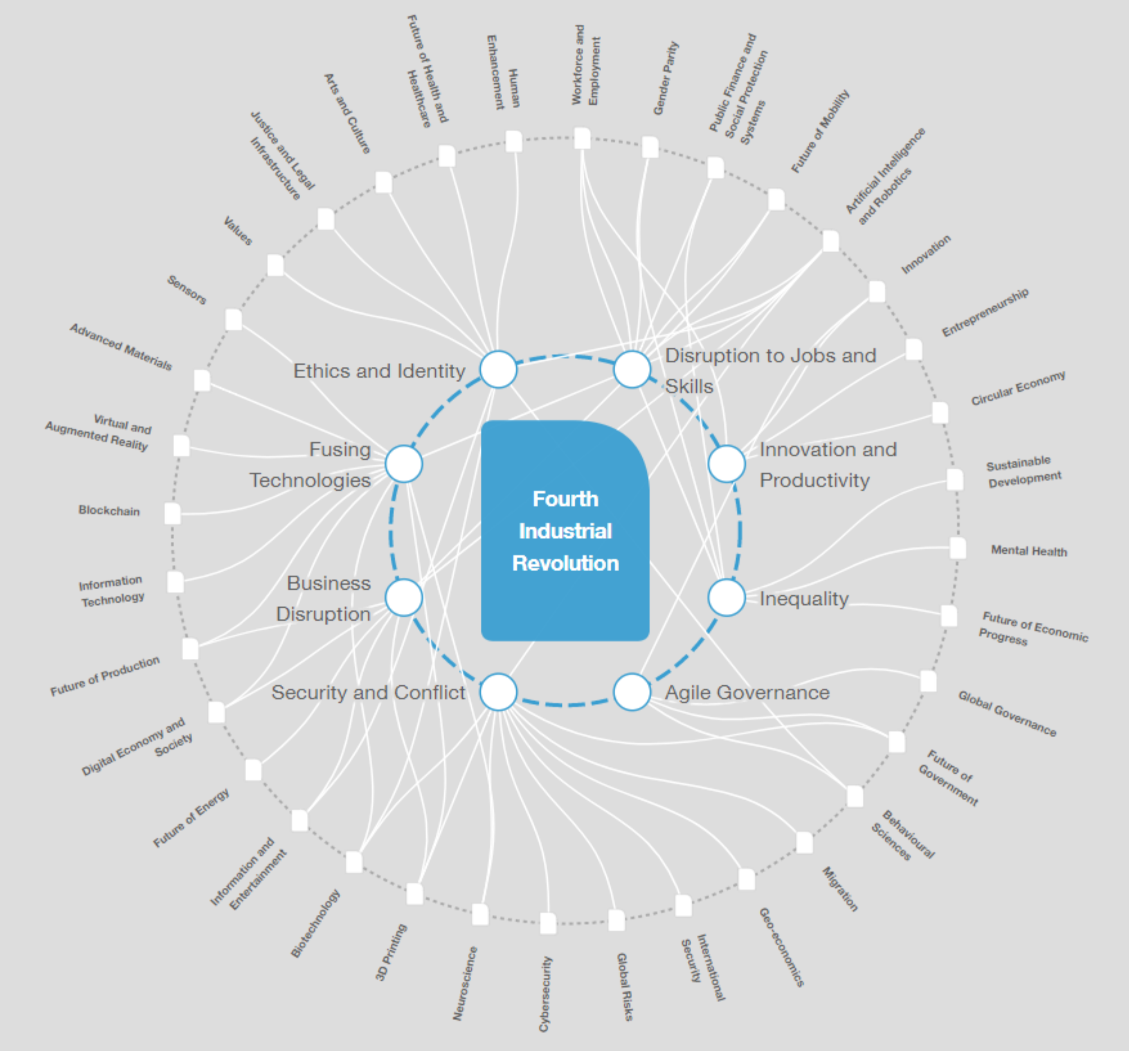
Leadership **&** **Knowledge**

WEF 2025 Megatrends

Physical **Digital** **Biological**

Megachanges of Industry 4.0.:

- Disruption of Jobs and Skills
- Innovation and Productivity
- Inequality
- Agile Governance
- Security and Conflict
- Business Disruption
- Fusing Technologies
- Ethics and Identity



© World Economic Forum

(cyber)Security and Conflicts

will be caused by insights from migration, new forms of government, international security cooperation, global risks, threats of cybersecurity, neuroscience, AI and robotics and bioengineering.

97,5%

of threats to cybersecurity are caused by human

-George C. Marshall Center - European Center for Security Studies

99,9%

of threats to information security are caused by human©

CyberSecurity VS Information Security

How Ukraine address the modern hybrid threats?

“...Ukraine has been at the forefront of counteracting Russian information warfare. The country experienced the impact of Russian propaganda, disinformation and hybrid war earlier than many other European or American societies. This makes the Ukrainian experience so unique and so informative ...”
Words and Wars (2017)

The national law ‘on the basic principles of ensuring cyber security of Ukraine’ defined the cybersecurity as ‘***safety of the vital interests of human and citizen, society and state when using cyberspace*** in case of which sustainable development of information society and the digital communication environment, timely identification, prevention and neutralization of real and potential **hazards of national security**’.

Information Security Doctrine of Ukraine *as 'counteraction'*

main goal of it was setting ground rules of national information policy to resist the weaponized information impact from Russian Federation in a state of acting **hybrid war**.

the document it considers:

creation of an integrated system of evaluation of informational threats;

increasing regulatory efficiency of state authorities engaged in information space governance;

legal mechanism searching, estimating, blocking and deleting from information space of state (not only internet), and from Ukrainian segment of the internet*

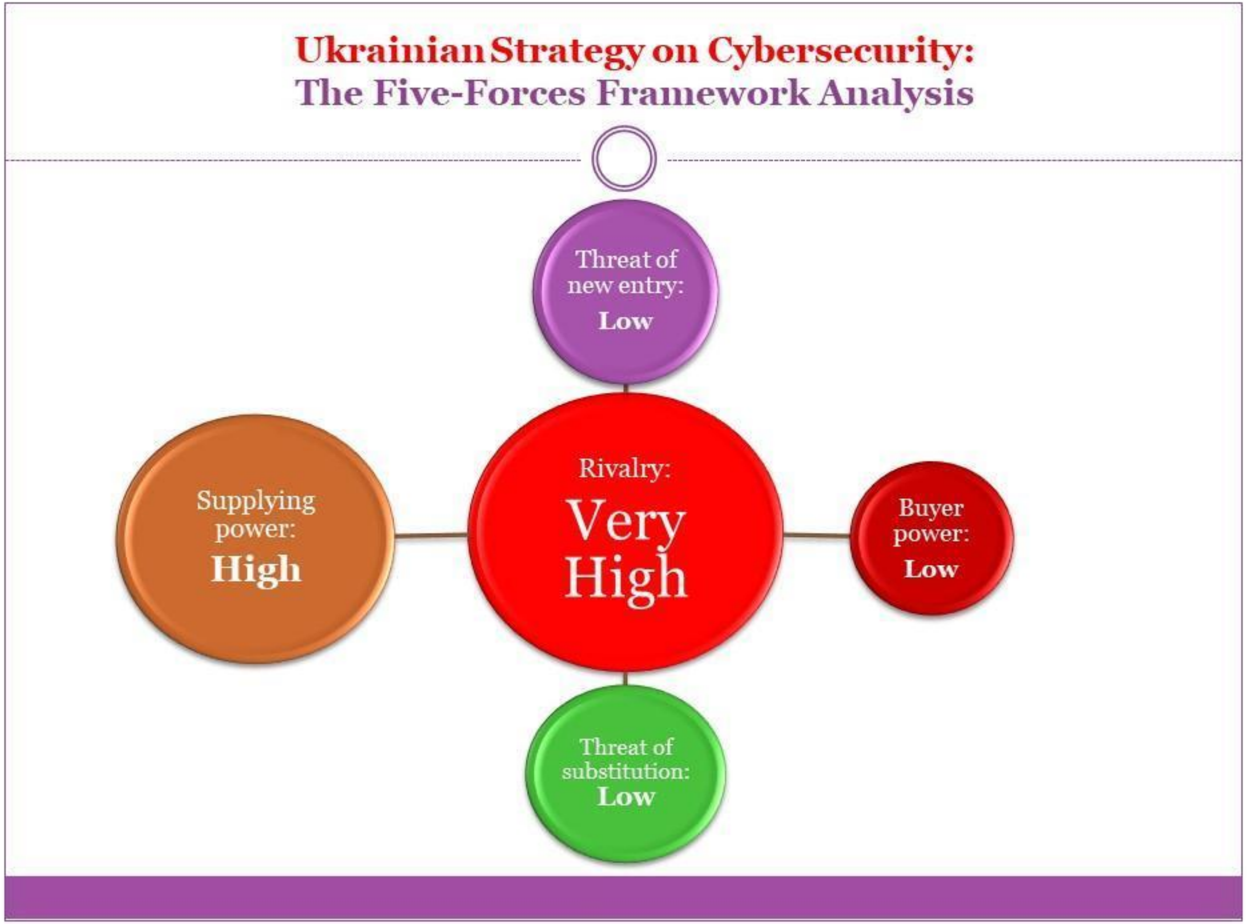
defines work of telecom, media and press during state of war;

cooperation with civil society to combat information aggression, disinformation and propaganda;

safeguarding international image and reputation of Ukraine.

Five forces of CyberCompetetiveness of *Ukraine*

The Five-Forces on Strategy on Cybersecurity Strategy showed high influents of rivalry and dependency on cybersecurity solution suppliers. The strategy has implemented needed framework for ***coordination between key stakeholders***, what let to examine the strategy to be *sufficient and up to date.*



Ukrainian Strategy on Cybersecurity:
The Five-Forces Framework Analysis

Threat of new entry: **Low**

Supplying power: **High**

Rivalry: Very High

Buyer power: **Low**

Threat of substitution: **Low**

The basic elements of the Cyber Security Framework in *Georgia*

- Law of Georgia on Information Security, 2012
- National Security Concept of Georgia, 2014
- Cyber Security Strategy of Georgia, 2012-2015
- New Cybersecurity Strategy of Georgia, 2016
- Cybersecurity Strategy of Georgia, 2017-2018

Cyber Security and Information Security in *Georgia*

Law of Georgia on Information Security *defines:*

- **information security** – an activity that ensures the protection of access to, integrity, authenticity, confidentiality, and non-repudiation of ***information and information systems***;

- **information security policy** – a set of the standards, principles, and practices laid down in this Law, other normative acts and international treaties of Georgia, that ensures information security and complies with the international standards established within the scope of its maintenance;

Key Objectives and Principles of Cybersecurity Policy of Georgia:

- Cybersecurity as the integral part of the national security

- Uncompromised protection and respect for the human rights and basic freedoms

- Common approach of the Government of Georgia

- Collaboration between the state and private sectors
- Active international cooperation –

- Individual responsibility

- Adequate measures

Information security

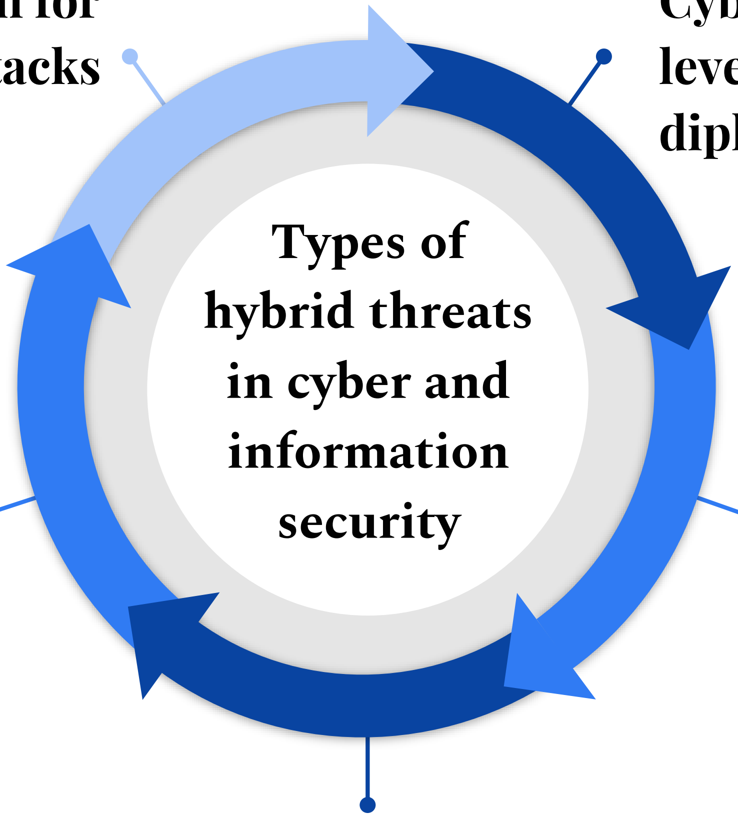
definition

AS system on **state governed actions** of the ***information flows*** into social consciousness with for safeguarding nation (citizens and residents) from ***weaponized influence*** from **internal** and **external threats** in form of ***propaganda, disinformation, violent ideologies, aggressive and disruptive social phenomena***.

Defining ‘Hybrid threats’

‘Hybrid threats can range from cyberattacks on critical information systems, through the disruption of critical services such as energy supplies or financial services, to the undermining of public trust in government institutions or the deepening of social divisions.’*

- *European Parliament And The Council on Joint Framework on countering hybrid threats, 2016*



Types of hybrid threats in cyber and information security

Retaliation for cyber attacks

Cyber leverages to diplomacy

Cyber sabotage and espionage

Propaganda

Cyber troops, weapons and arm race

Conclusion

Spread and wide use of the Internet - something unexpected yet influential, making it one of Nassim Taleb's '**black swans**' - apparently caught the world off-guard. Politics, law and security **have not yet came up with a *matching response***.

RACI
RIPE Academic Cooperation Initiative

Q & A

Oleksandr Tsaruk and Maria Korniiets

Annexes

Year Actor	2013	2014	2015	2016	2017	2018
Non-state	- Mar: ”the largest publicly announced DDoS attack in the history of the Internet.” -Nov: ’Anonymous’ group Singapore hack.	-Jun: World Cup in Brazil threats by ‘Anonymous’ group.	-Jan: US military social media hacked by ISIS sympathizers.	-Aug: ‘Shadow Brokers’ group claims to have stolen US NSA data.	-Jul: Equifax credit bureaus breach; -Sep: Attack on U.S. Securities and Exchange Commission; -Oct: Hackers target schools threatening to release private records unless paid.	-Feb: Olympic Destroyer' malware attack confirmed; -Jan: India national database with citizen biometrical data stolen.

Table 1. Prominent cyber and information security breaches (part 2)

Year Actor	2013	2014	2015	2016	2017	2018
State	- Jan: The New York Times hacking attempt blamed on China; -Mar: South Korea media and banking attack; -Jun: South Korea government website hack; -Jun: Israel accuses Iran of non-stop attacks on computer systems.	- Mar: Ukraine accuses Russia of compromising mobile network; -Jul: Dragonfly cyber espionage discovered; -Nov: Sony Pictures hack; -Nov:US Post hacked; -Nov: Regin spyware discovered; -Dec:South Korea nuclear plant compromised; - Dec: Kenya arrests 77 Chinese citizen accused of running a cybercrime center.	-Feb: SIM cards producer company Gemalto hack; -Feb: alleged cyberattack on Sony Pictures Entertainment by North Korea; -Jun: German parliament cyber attack; - Jun: US federal employees data breach (the ‘OPM’ hack).	-Mar: Petya malware; -US presidential election: - Jun: The Democratic National Committee files exposed; - Dec: US Department of Homeland Security accused of trying to access state of Georgia election database. -Jul: Russian Federal Security Service reports a "professional" cyber attack; - Sep and Dec: ‘State-sponsored’ attacks on Yahoo; - Dec: FBI investigates FDIC hack.	- Apr: US NSA breach; - May: WannaCry ransomware attack discovered, hitting 150 countries; - May: Emmanuel Macron's data leak in wake of French election; - Jun: NotPetya ransomware attacks major companies; -Jun: US voters information leak; -Oct: Bad Rabbit ransomware (mainly Russia and Ukraine); -Dec: the plants in the Middle East were stopped by a Triton malware attack.	-Mar: Cambridge Analytica scandal(US and Nigeria election); -Mar:Russian Government Cyber Activity Targeting Critical Infrastructure Sectors; - Sep: UEFI Rootkit LoJax (“the hackers’ Holy Grail”) discovered in use; - Oct: Bloomberg ‘Big Hack’ story;-Dec: Marriott hotel chain database compromised.

Table 1. Prominent cyber and information security breaches (part 1)