Interviewer: Could you please tell us a bit about yourself and what you do?

Researcher: I'm the Deputy Dean of the Faculty of Informatics at Kyiv-Mohyla Academy. I work as a consultant in cybersecurity, digital transformation, and development. You could call me an IT generalist.

Interviewer: How has Ukraine's cyber situation changed since the beginning of the full-scale invasion?

Researcher: Obviously, the number of cyberattacks has increased because it became a priority for Russia. But Russia has been actively attacking us for years. What's changed is that they've removed any remaining barriers.

Russians are trying to scale their activities by involving more participants and creating the impression of widespread activity. Recent research suggests that hacker groups like "Sun Spitter" are actually the same GRU operatives (Russian military intelligence) creating multiple identities to generate the impression of larger numbers.

There are real consequences though. Putin has attempted to pass laws seemingly for ethical hacking to improve cybersecurity, but in reality, there's no such thing as private cybersecurity in Russia. Anyone working in cyber in Russia, especially professionals, is with about 80% probability pro-government at minimum.

The interest in targeting Ukraine has grown significantly, and so has the activity. Previously, they tried to be somewhat discreet, but now there are no limitations - they do whatever they can.

Interviewer: What lessons has the cybersecurity community learned from attacks on Ukraine's infrastructure, and how can hospitals prepare for similar threats?

Researcher: The most important shift is that everyone now operates within a cybersecurity framework. We use the term "cyber resilience." This approach recognizes that we can't have protected government entities and vulnerable private companies, or vice versa. There's a unified country framework where if any link is vulnerable - whether state or private business - everyone loses.

Now the government actively helps private, non-cyber businesses like retail stores or Nova Poshta (postal service), and conversely, private tech businesses try to help the state improve its cyber culture.

For hospitals specifically, you should know that Russia hacked Okhmatdyt Children's Hospital's network before a missile strike. Hospitals face similar cybersecurity needs as others, but the criticality is different. An hour of internet outage for a private company is one thing; for a hospital, it's entirely different.

Hospitals should prepare as critical infrastructure. I recommend non-cyber professional organizations adopt a zero-trust architecture approach - looking at each component of your digital infrastructure asking "what if this node or element gets compromised?" Based on this approach, create an action plan and basic countermeasures.

The current trend in cyber operations is not just about detecting potential breaches but understanding how quickly you can recognize you've already been compromised. Focus less on cybersecurity and more on detecting network intrusions.

Interviewer: Russia's cyber warfare tactics have included attacks on energy networks, communications, and critical infrastructure. How might these tactics be adapted for attacks on medical institutions?

Researcher: This is a sensitive topic that the Red Cross has been trying to address in the context of cyber warfare. Cyber operations can be categorized by their consequences. Some directly impact military outcomes - for example, if they breach the Ministry of Defense systems affecting logistics.

Others have political motives. When ministries were hacked and registries stopped working, it wasn't just about the registries themselves - it's about how society perceives this. There's a theory of sabotage that applies here. These attacks have both physical and mental effects on society.

Imagine a hospital gets hacked and equipment stops working entirely. What's the result? In terms of conventional warfare, it might affect a few hundred people - not enough to significantly impact the war effort. But the moral effect would be much greater because it strongly affects society, raises fear, and undermines trust in the medical system. People will wonder if they should go to a hospital where they might die because devices stop working.

Cyber operations by themselves are rarely decisive - they complement other actions. They're auxiliary tools in the context of a full-scale war, supplementing other military-political objectives. They're rarely self-sufficient activities because on their own, they have limited impact.

Interviewer: What role does malware play in the conflict in Ukraine, and how can this threat affect society's security?

Researcher: Your question hits the mark because Russia isn't exceptionally strong in offensive cyber capabilities when it comes to finding vulnerabilities and exploiting them. However, they excel at social engineering and developing viruses.

This is one of their key tools, and they have good Researchers in virus development. Just consider Kaspersky Lab and what that represents - those who develop security systems must understand how things work. Russia effectively combines social engineering attacks with viruses. Remember how many examples there are of Ukrainian citizens finding fake packages, voting machines in Telegram, or other scams. This is one of their most effective tools.

Interviewer: Which cyber warfare tactics like wiper malware, DDoS attacks, and phishing campaigns are most likely to be used against critical infrastructure, and how can they be countered?

Researcher: DDoS attacks are unlikely to be effective on their own. There was one case when hackers targeted Zakarpattiaoblenergo (regional energy company), complementing their operation by flooding their hotline with calls.

Phishing and malware are all forms of social engineering. Phishing is a tool to obtain someone's password, but you can't "hack with phishing" directly - you need to establish contact with a person first and then try to send them a malicious link. The same applies to viruses - they can't magically materialize on a computer; someone needs to launch them. This is where Russians are particularly active and effective, spreading viruses through phishing.

International Cyber Threats

Interviewer: Which countries or hacker groups pose the greatest cyber warfare threats to Ukraine's critical infrastructure?

Researcher: You need to understand that very few states officially acknowledge their cyber forces. Even those that do rarely provide any information. I recommend looking into the Stuxnet virus - there are books and documentaries about it. This operation disrupted Iran's nuclear reactor development. The physical site was heavily protected, so they compromised it with a virus. The operation happened around 2014, but to this day, no one has claimed responsibility.

We have significant problems with international legislation regarding cyber warfare. If you carefully read the law, the concept of "cyber war" doesn't officially exist.

The main threats come from rogue states that don't hide their efforts and those who make money from it, like North Korea with the Lazarus Group. Iran wants to be effective but can't achieve systematic results, occasionally having some minor successes. China is also quite capable in terms of cyber operations.

In terms of activity, China would be the most active, followed by Russia, North Korea, and Iran. Interestingly, only North Korea and Iran acknowledge their cyber forces, and I'm not even sure North Korea does.

Interviewer: How has Ukraine's cooperation with Western countries in cybersecurity affected the geopolitical balance?

Researcher: Cybersecurity operations don't have a clearly pronounced kinetic effect. If Ukrainian operations exist at all, they likely don't have significant impact. The SBU (Security Service of Ukraine) and the GUR (Defense Intelligence) have acknowledged some supposed hacker groups, but if you carefully read what they've claimed, it's often not very substantial.

If you ask "so what happened?" after reading news that someone hacked something, it becomes clear that either cyber warfare doesn't really exist, or the results aren't visible. We'll either see results on the battlefield without connecting them to cyber operations, or we'll see effects in our fellow citizens' minds in the form of "they hacked our registries - how terrible."

Interviewer: What role does cyber warfare play in modern hybrid warfare strategy?

Researcher: Currently, it doesn't play an adequate role, but I think in the future, alongside drones, it will become one of the pillars of full-scale warfare. But for now, it's still being tested. Even drones, despite all our impressive achievements, are only at the beginning of their technological development. I think something similar will happen with cyber operations - we should expect new developments about cyber involvement in various operations.

Interviewer: Ukraine has received international assistance in cybersecurity, particularly from NATO and private companies like Microsoft and Google. How important is external cooperation for the resilience of critical infrastructure cybersecurity?

Researcher: It's extremely important because of what we call "threat snowballing." Even if there were some hypothetical peace, you don't see who's "cyber shooting" or not. This remains an open question.

Let me explain with a practical example about hacker groups and their tactics, techniques, and procedures (TTPs). Non-ultra-professional hacker groups tend to use similar attack patterns. If a hacker group X attacked company Y in country Z, and there's no international exchange of information, then nothing interesting happens. But if there's international exchange of intelligence about attacks, this information is instantly distributed to all other countries, and threat hunting begins. You know in advance that there's a high probability your system will face similar actions, likely from a specific group, allowing you to counter it effectively.

Interviewer: Ukraine has entered a more digitalized era. We use "Diia" to store our documents, and most citizens abroad use it as their main infrastructure for accessing documents. How resistant is Diia?

Researcher: The Ministry of Digital Transformation is making maximum efforts to ensure the highest level of protection for Ukrainians' personal data and digital security within Diia.

Interviewer: In Denmark, they have a program called MitID for digital signatures. Would it be possible to create a similar authentication system in Ukraine?

Researcher: We already have this with BankID. If you're a client of many banks, you have your digital BankID that you can use to sign documents and authorize on some government services. Diia also has signature capabilities and other features.

Interviewer: What if we implemented a system in Ukraine where each person has their individual number linked to documents and medical records? Would that be possible in the future?

Researcher: We already have that now. Diia collects all documents together. I personally have my international passport, internal ID, two diplomas, vehicle registration - it's already essentially in place.

Interviewer: How resistant is Diia to cyberattacks and identity theft?

Researcher: The developers and support teams for Diia follow the best global cybersecurity practices to ensure the highest level of protection.