WEBVTT

00:00:04.300 --> 00:00:09.100
<v SPEAKER_1>In today's episode of Defence Deconstructed, which we're recording on the 26th of November, we're talking to Dr.

00:00:09.100 --> 00:00:20.360
<v SPEAKER_1>Julie Kim, our postdoctoral fellow leading the career program at the Canadian Global Affairs Institute to talk about her new paper From Intelligence Gathering to Financial Gain, Countering DPRK Cyber Operations.

00:00:20.360 --> 00:00:33.020
<v SPEAKER_1>Julie and I talk about North Korea's cyber and IT capabilities, how the country produces them despite its isolation from the rest of the world, its hacking capabilities and the work of Canada and its allies in monitoring and countering these activities.

00:00:33.020 --> 00:00:41.420
<v SPEAKER_1>One final note for me, this coming Tuesday, December 2nd, is Giving Tuesday, which is an important day in the calendar for registered charities like the Canadian Global Affairs Institute.

00:00:41.420 --> 00:00:48.440
<v SPEAKER_1>If you enjoy this podcast, one of the ways you can support it is by visiting our website and donating through the support CGAI link.

00:00:48.440 --> 00:00:54.220
<v SPEAKER_1>All your donations will be eligible for a 100% CRA charitable donation tax receipt.

00:00:54.220 --> 00:00:55.680
<v SPEAKER_1>Thanks in advance for your consideration.

00:01:01.730 --> 00:01:04.350
<v SPEAKER_1>Julie, welcome back to Defence Deconstructed.

00:01:04.350 --> 00:01:06.550
<v SPEAKER_2>Thanks for having me again.

00:01:06.550 --> 00:01:11.270
<v SPEAKER_1>So we've got you on here today to talk about another recent paper that you've published with us.

00:01:11.270 --> 00:01:18.610
<v SPEAKER_1>This one's titled From Intelligence Gathering to Financial Gain, Countering DPRK Cyber Operations.

00:01:18.610 --> 00:01:25.650

<v SPEAKER_1>Just to start this conversation, can you give us a bit of an overview and some of the context for how we should be thinking about what North Korea does in the cyber domain?

00:01:27.630 --> 00:01:29.090
<v SPEAKER_2>Sure.

00:01:29.090 --> 00:01:38.550
<v SPEAKER_2>So even if you're not that familiar with the North Korean regime, you've probably heard about some of their cyber attacks, like the one on Sony back in 2014.

00:01:39.610 --> 00:01:47.150
<v SPEAKER_2>North Korea has built a pretty aggressive cyber program over the years, and it's now become a serious global security concern.

00:01:47.150 --> 00:01:51.610
<v SPEAKER_2>In the early days, their cyber attacks were mostly politically motivated.

00:01:51.610 --> 00:01:57.110
<v SPEAKER_2>They were focused on collecting intelligence and learning how its adversaries operate.

00:01:57.110 --> 00:02:02.670
<v SPEAKER_2>So their key targets included government officials, academics, and journalists.

00:02:02.670 --> 00:02:13.450
<v SPEAKER_2>And they also targeted defence companies to steal sensitive information on weapons development, especially technologies related to satellites and semiconductors.

00:02:13.450 --> 00:02:21.430
<v SPEAKER_2>But the scope of North Korea's operations changed dramatically after the UN imposed sanctions in response to its nuclear test.

00:02:22.170 --> 00:02:26.630
<v SPEAKER_2>After that, their operations expanded heavily into financial crime.

00:02:26.630 --> 00:02:38.010
<v SPEAKER_2>And so despite multiple international sanctions, North Korea continues to fund its weapons of mass destruction and ballistic missile programs through illicit cyber activities.

00:02:38.010 --> 00:02:43.990
<v SPEAKER_2>That includes money earned by overseas IT workers and large-scale financial theft.

00:02:43.990 --> 00:02:48.550
<v SPEAKER_2>And in this paper, I focused mainly on these IT workers and cyber espionage.

00:02:49.330 --> 00:02:54.070
<v SPEAKER_2>Over the past decade, we've seen North Korea really grow its cyber capabilities.

00:02:54.070 --> 00:02:56.670
<v SPEAKER_2>And the hackers have become a lot more innovative.

00:02:56.670 --> 00:03:06.770
<v SPEAKER_2>They're integrating new technologies, leveraging AI to identify targets, and employing social engineering tactics to make their attacks more effective.

00:03:06.770 --> 00:03:15.190
<v SPEAKER_2>So even though there are ongoing efforts to strengthen international cyber security cooperation, there are still major challenges ahead.

00:03:15.730 --> 00:03:25.190
<v SPEAKER_1>So, given that the North Korean regime is incredibly isolated, it might be a bit hard for people to have an insight into what's actually happening inside the country.

00:03:25.190 --> 00:03:31.950
<v SPEAKER_1>But from what you've described, it does seem like they've made a significant investment in development of IT capabilities.

00:03:31.950 --> 00:03:39.290
<v SPEAKER_1>How does the North Korean government actually do that and have technical proficiency if it's so isolated from the international community?

00:03:39.290 --> 00:03:43.490
<v SPEAKER_2>So North Korea has actually been investing in science and technology for decades.

00:03:43.710 --> 00:03:46.730
<v SPEAKER_2>And information technology is a big part of that.

00:03:46.730 --> 00:03:57.450
<v SPEAKER_2>The state invests heavily in fostering young talent through a highly competitive education system where only the top students are admitted into elite science and technology programs.

00:03:57.450 --> 00:04:01.530
<v SPEAKER_2>Students are identified at a young age from elementary or

middle schools.

00:04:01.530 --> 00:04:12.510
<v SPEAKER_2>And among them, the top students are selected to study computer science at elite universities in Pyongyang, such as Kim Il Sung Military University or Kimchek University of Technology.

00:04:13.370 --> 00:04:18.830
<v SPEAKER_2>And some of them even get opportunities to study or train abroad in China or Russia.

00:04:18.830 --> 00:04:25.170
<v SPEAKER_2>And when they graduate, most of them go on to work in government agencies or state-run IT organizations.

00:04:26.210 --> 00:04:35.930
<v SPEAKER_2>And while it's never been officially confirmed, the Reconnaissance General Bureau is widely seen as the main institution driving North Korea's cyber program.

00:04:37.310 --> 00:04:44.970
<v SPEAKER_2>The regime regularly reorganizes it, restructuring or creating new units to meet its strategic needs.

00:04:44.970 --> 00:04:50.490
<v SPEAKER_2>And today, North Korea's elite cyber force is believed to be around 7,000 hackers.

00:04:50.490 --> 00:04:54.850
<v SPEAKER_2>And these are the people who handle the most complex and sensitive operations.

00:04:54.850 --> 00:05:02.290
<v SPEAKER_2>Then you have a much larger number of ordinary IT workers who do more mundane tasks while hiding their North Korean identities.

00:05:03.410 --> 00:05:11.730
<v SPEAKER_2>And one of the biggest recent developments is the creation of a new AI research center in March 2025.

00:05:11.730 --> 00:05:22.610
<v SPEAKER_2>Its purpose is to strengthen offensive cyber capabilities, everything from developing advanced hacking tools to using AI for information theft and data collection.

00:05:22.610 --> 00:05:29.630
<v SPEAKER_2>And shortly after the center was set up, state media announced the launch of a new AI-enabled suicide drone.

00:05:30.210 --> 00:05:39.730

<v SPEAKER_2>So what we're seeing is the integration of AI into both cyber operations and military systems, which is raising serious concerns in the international community.

00:05:41.290 --> 00:05:46.190
<v SPEAKER_1>So you've been talking about the different workers, their skill sets.

00:05:46.190 --> 00:05:51.350
<v SPEAKER_1>What kind of work specifically do they do and how do they actually operate in doing it?

00:05:52.910 --> 00:06:01.270
<v SPEAKER_2>North Korea sends thousands of highly skilled IT workers abroad, and their main job is to basically make money for the regime.

00:06:01.270 --> 00:06:11.930
<v SPEAKER_2>Their earnings are a major source of funding for North Korea's economic and security priorities, including its weapons of mass destruction and ballistic missile programs.

00:06:11.930 --> 00:06:21.830
<v SPEAKER_2>The government actually sets annual revenue quotas for these workers, and each organization must fund themselves while also meeting their revenue targets.

00:06:21.830 --> 00:06:31.070
<v SPEAKER_2>These quotas are believed to be the main driving force behind IT workers, and their diversification and expansion into new cybercrimes.

00:06:31.070 --> 00:06:38.890
<v SPEAKER_2>And because North Korea's domestic internet infrastructure is so limited, a lot of these operations actually happen outside of the country.

00:06:38.890 --> 00:06:45.650
<v SPEAKER_2>And most of these workers are based in China and Russia, with smaller numbers in Southeast Asia and Africa.

00:06:45.650 --> 00:06:47.210
<v SPEAKER_2>They hide their identities.

00:06:47.210 --> 00:06:57.390
<v SPEAKER_2>They use forged resumes, passports, diplomas and bank documents to land freelance contracts with companies around the world, including in North America and Europe.

00:06:57.390 --> 00:07:03.650
<v SPEAKER_2>And once they win the contracts, they receive payment in

cryptocurrency, so the money can't be easily tracked.

00:07:03.650 --> 00:07:10.350
<v SPEAKER_2>In 2024, a UN report estimated that they bring in up to $600 million a year.

00:07:10.350 --> 00:07:16.950
<v SPEAKER_2>And in addition to hosting IT workers, China and Russia sometimes also help facilitate their activities.

00:07:16.950 --> 00:07:23.850
<v SPEAKER_2>For example, some Chinese companies have acted as fronts, helping North Koreans secure jobs or bypass sanctions.

00:07:24.670 --> 00:07:33.870
<v SPEAKER_2>And in Russia, some companies were sanctioned by the US after hiring North Korean IT workers under a 10-year contract.

00:07:33.870 --> 00:07:37.310
<v SPEAKER_2>Southeast Asia is another important hub.

00:07:37.310 --> 00:07:44.210
<v SPEAKER_2>And in one case, Cambodia even granted citizenship to North Koreans who are violating sanctions.

00:07:44.210 --> 00:07:48.410
<v SPEAKER_2>And now as for what these workers actually do, it's a pretty wide range.

00:07:48.410 --> 00:07:57.530
<v SPEAKER_2>They create mobile and web applications, design games, work on animation or graphics, and even take on AI-related projects.

00:07:57.530 --> 00:08:06.230
<v SPEAKER_2>They usually work remotely, hide their real identities, sometimes through subcontractors who set up laptop farms with clean IP addresses.

00:08:06.230 --> 00:08:13.390
<v SPEAKER_2>And they'll use VPNs or third country networks to make it look like they're actually logging in from somewhere else.

00:08:13.390 --> 00:08:25.130
<v SPEAKER_2>And with remote work becoming so common, and with AI making it easier to fake identities, the risk of accidentally hiring a North Korean IT worker has grown significantly.

00:08:25.130 --> 00:08:27.970
<v SPEAKER_2>And Canada isn't immune to this.

00:08:27.970 --> 00:08:36.070
<v SPEAKER_2>In July this year, the RCMP issued an advisory warning Canadian businesses about the risks of hiring North Korean IT workers.

00:08:36.070 --> 00:08:44.750
<v SPEAKER_2>So it's becoming really important for companies to strengthen their hiring processes and for governments to provide clear guidance to help them do that.

00:08:47.010 --> 00:08:50.430
<v SPEAKER_1>This episode of Defence Deconstructed is brought to you by Irving Shipbuilding.

00:08:50.430 --> 00:08:52.950
<v SPEAKER_1>Canada's national shipbuilder is currently hiring.

00:08:52.950 --> 00:08:57.950
<v SPEAKER_1>For more information on the many jobs and opportunities currently available, please visit www.shipsforcanada.ca.

00:09:03.870 --> 00:09:13.930
<v SPEAKER_1>So we often hear about various different hacking efforts by North Korea that target academics, journalists, government officials, and either South Korea or the United States.

00:09:13.930 --> 00:09:18.970
<v SPEAKER_1>But could you maybe walk us through some of the more recent operations to give a bit more sense of the specifics?

00:09:20.650 --> 00:09:21.910
<v SPEAKER_2>Yeah, sure.

00:09:21.910 --> 00:09:24.910
<v SPEAKER_2>North Korean hackers are very active in cyber espionage.

00:09:24.910 --> 00:09:31.730
<v SPEAKER_2>And basically, their main goal is to gather intelligence that supports the regime's strategy goals.

00:09:31.730 --> 00:09:38.550
<v SPEAKER_2>They mostly go after targets in South Korea and the United States, government officials, military personnel, and academics.

00:09:39.310 --> 00:09:44.710
<v SPEAKER_2>And in the past, they also targeted Russian defense companies to steal military technology.

00:09:44.710 --> 00:09:53.810
<v SPEAKER_2>But it's unclear whether that's still happening now that

North Korea and Russia have strengthened their relationship under the Comprehensive Strategy Partnership in 2024.

00:09:56.110 --> 00:10:01.390
<v SPEAKER_2>There are a few major groups behind these operations, and each one has a different mission.

00:10:01.390 --> 00:10:05.170
<v SPEAKER_2>One of the most active is Kim Sook-hee, also known as APT 43.

00:10:05.950 --> 00:10:10.470
<v SPEAKER_2>They focused on collecting intelligence on geopolitical events and foreign policy.

00:10:10.470 --> 00:10:16.030
<v SPEAKER_2>So they tend to target governments, think tanks, universities and media.

00:10:16.030 --> 00:10:26.550
<v SPEAKER_2>And another group, Andariel or APT 45, goes after sensitive technical information that could support North Korea's military and nuclear programs.

00:10:26.550 --> 00:10:31.710
<v SPEAKER_2>So their targets are usually in defense, aerospace, engineering and nuclear sectors.

00:10:32.830 --> 00:10:43.110
<v SPEAKER_2>In terms of broader trends, foreign governments still remain the number one target, followed by cryptocurrency, media, finance, defense and NGOs.

00:10:43.110 --> 00:10:53.930
<v SPEAKER_2>And to give you a recent example, between March and July this year, North Korea linked hackers carried out at least 19 spear phishing attacks against foreign embassies in South Korea.

00:10:53.930 --> 00:11:04.710
<v SPEAKER_2>They pretended to be diplomats and sent very convincing emails with official letters, event invitations, things that embassies that would normally expect to receive.

00:11:04.710 --> 00:11:09.710
<v SPEAKER_2>That operation is believed to be tied to Kintsuki with potential links to China.

00:11:09.710 --> 00:11:28.650
<v SPEAKER_2>That is because a cyber security firm later found that the activity matched closely with Chinese time zone and working hours,

and even paused during major Chinese national holidays, not North Korean ones, that suggests the group may be operating from inside China or relying on Chinese resources.

00:11:28.650 --> 00:11:34.570
<v SPEAKER_2>And beyond espionage, North Korean hackers also run psychological operations.

00:11:34.570 --> 00:11:46.250
<v SPEAKER_2>They impersonate foreign media outlets to create fake news about sensitive political or economic issues, and push that content across social media to create public discord.

00:11:46.250 --> 00:11:55.770
<v SPEAKER_2>Now all of this shows how persistent and evolving North Korea's cyber operations are, and why closer international cooperation is so crucial to countering them.

00:11:59.350 --> 00:12:10.410
<v SPEAKER_1>So lastly, could you talk about recent efforts that we've seen in the international space in terms of cyber security cooperation that's trying to get at and deal with North Korean cyber activities?

00:12:10.630 --> 00:12:16.050
<v SPEAKER_1>And in conjunction with that, what is Canada doing in collaboration with allies in this respect?

00:12:18.190 --> 00:12:21.330
<v SPEAKER_2>First of all, cyber threats don't just stop at borders.

00:12:21.450 --> 00:12:26.470
<v SPEAKER_2>So countries need to establish systems for intelligence sharing and joint exercises.

00:12:26.470 --> 00:12:37.230
<v SPEAKER_2>It's also increasingly important for governments and the private sector to share information quickly, because many cyber incidents are first detected by industry, not by governments.

00:12:37.230 --> 00:12:43.950
<v SPEAKER_2>And since South Korea is the main target of North Korea cyber operations, the country is on the front lines of this issue.

00:12:43.950 --> 00:12:56.550
<v SPEAKER_2>And according to the National Intelligence Service of Korea, about 80% of all cyber attack attempts against South Korea's public sector in 2023 were linked to North Korea.

00:12:56.550 --> 00:13:00.190
<v SPEAKER_2>That's roughly 1.3 million attempts per day.

00:13:00.190 --> 00:13:13.330
<v SPEAKER_2>In response, Seoul has strengthened its institutions, including establishing the National Cyber Crisis Management Center, and also deepened cooperation with key allies and international organizations.

00:13:13.330 --> 00:13:16.790
<v SPEAKER_2>One major development is South Korea's growing partnership with NATO.

00:13:17.610 --> 00:13:24.530
<v SPEAKER_2>Since 2021, Korea has taken part in NATO's annual cyber defense exercise Locked Shields.

00:13:24.530 --> 00:13:31.770
<v SPEAKER_2>In 2022, it became the first Asian country to join the NATO Cooperative Cyber Defense Center of Excellence.

00:13:31.770 --> 00:13:42.950
<v SPEAKER_2>And in 2023, South Korea and NATO signed an enhanced partnership, the Individually Tailored Partnership Program, that expands cooperation in cyber defense and emerging technologies.

00:13:44.150 --> 00:13:49.370
<v SPEAKER_2>South Korea has also expanded bilateral and trilateral cooperation with the United States.

00:13:49.370 --> 00:13:55.850
<v SPEAKER_2>For instance, it launched the ROK-US Strategic Cyber Security Cooperation Framework.

00:13:55.850 --> 00:14:07.130
<v SPEAKER_2>And later in 2023, South Korea, the US and Japan held their first trilateral cyber dialogue focused on countering North Korean cyber activities.

00:14:08.270 --> 00:14:11.810
<v SPEAKER_2>Now on the Canadian side, we're seeing more engagement in the Indo-Pacific.

00:14:12.510 --> 00:14:18.830
<v SPEAKER_2>Canada has identified cyber security cooperation as a key component of its Indo-Pacific strategy.

00:14:18.830 --> 00:14:36.670
<v SPEAKER_2>And as part of that initiative, it announced the Cyber Security and Digital Technology Diplomacy Project, which allocates $47.4 million over five years to enhance cyber capacity in partner countries and also increase regional engagement through the deployment

of cyber attaches.

00:14:37.650 --> 00:14:43.790
<v SPEAKER_2>And the new Canadian Armed Forces Cyber Command, CAF Cybercom, is also taking a more active role.

00:14:43.790 --> 00:14:48.470
<v SPEAKER_2>And in fact, Canada and South Korea have had a particularly active year this year.

00:14:48.470 --> 00:14:58.930
<v SPEAKER_2>In May, they participated as a team in exercise locked shields and later collaborated again during the APEC Cyber Defense Exercise at Cyber Summit Korea.

00:14:58.930 --> 00:15:09.570
<v SPEAKER_2>These are important steps towards strengthening not just bilateral cooperation, but also broader multilateral partnerships with other Indo-Pacific allies.

00:15:09.570 --> 00:15:20.430
<v SPEAKER_2>And finally, while North Korea isn't the biggest cyber threat to Canada compared to China or Russia, North Korea linked cybercrime is still a persistent risk for Canadian individuals and businesses.

00:15:20.710 --> 00:15:28.790
<v SPEAKER_2>So, Canada's continued cooperation with partners is essential for building collective resilience against shared threats.

00:15:31.390 --> 00:15:35.270
<v SPEAKER_1>Julie, thanks again for joining us to talk about your research for us.

00:15:35.270 --> 00:15:39.970
<v SPEAKER_1>Last question for you that you know you're going to get, what are you reading these days?

00:15:41.410 --> 00:15:44.870
<v SPEAKER_2>I actually just picked up a new book last weekend.

00:15:44.870 --> 00:15:49.950
<v SPEAKER_2>It's called Autocracy Inc, The Dictators Who Want to Run the World by Anne Applebaum.

00:15:51.050 --> 00:15:58.350
<v SPEAKER_2>I haven't started yet, so I can't give any impression so far, but I'm very interested in the topic.

00:15:58.350 --> 00:16:01.590

<v SPEAKER_2>Autocracy and dictatorships are my core research interest.

00:16:01.590 --> 00:16:08.430
<v SPEAKER_2>I wrote my PhD dissertation on it, The North Korean Regime Stability, and basically how the dictator survived.

00:16:08.430 --> 00:16:13.970
<v SPEAKER_2>So I'm really looking forward to reading this one and continue my academic interest.

00:16:13.970 --> 00:16:14.910
<v SPEAKER_1>Okay.

00:16:14.910 --> 00:16:17.630
<v SPEAKER_1>Thanks again, Julie, for joining us on Defence Deconstructed.

00:16:17.630 --> 00:16:18.230
<v SPEAKER_2>Thank you so much.

00:16:19.870 --> 00:16:22.030
<v SPEAKER_1>Thanks for listening to Defence Deconstructed.

00:16:22.030 --> 00:16:27.510
<v SPEAKER_1>For more of our work, go to cgai.ca or follow us on LinkedIn, Twitter, Instagram, or Facebook.

00:16:27.510 --> 00:16:34.090
<v SPEAKER_1>If you like what we do and want to keep us going, think of donating to us at cgai.ca slash support.

00:16:34.090 --> 00:16:36.690
<v SPEAKER_1>Defence Deconstructed is brought to you by our team in Ottawa.

00:16:36.690 --> 00:16:40.330
<v SPEAKER_1>Music credits go to Drew Phillips, and this episode was produced by Jordyn Carroll.