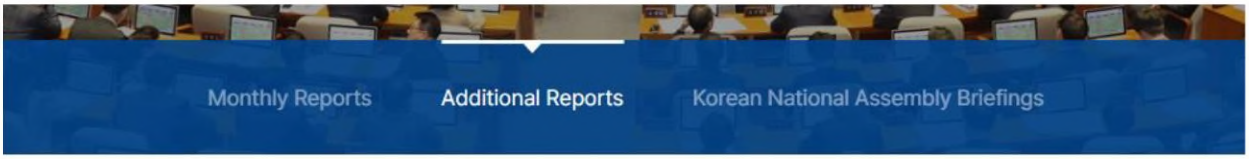
Oct 30_KIPEC Website_Expert Interview (Intelligence and Security Expert)

https://kipec.org/bsr/board.php?bo_table=archive&wr_id=12

https://kipec.org/ko/bsr/board.php?bo_table=archive&wr_id=12



KIPEC Focus: Expert Interview (Intelligence and Security Expert Edition)

2025-10-30 | 1

KIPEC Focus10302025.pdf

Expert Interview is a series that explores key developments in the United States through in-depth conversations with leading experts.

Our second interview featured Dr. Glenn Chafetz, Director of the 2430 Group, who brings over 30 years of government, academic, and private-sector experience. The discussion focused on North Korea's cyberstrategy and its implications for U.S.–South Korea security cooperation.

For further details, please refer to the attached report.

KIPEC 포커스: 전문가 대담 (정보·안보 전문가편)

2025-10-30 | 0

KIPEC 포커스10302025.pdf

KIPEC 포커스: 전문가 대담은 미국에서 발생하는 주요 사건에 대한 전문가를 인터뷰 하면서 그 현안을 알아보는 프로그램입니다.

두 번째 인터뷰로는 2430그룹(2430 Group)의 설립자이자 전무이사이며 정보·안보, 외교·국제정책, 지식재산 보호 및 디지털 관리 분야에서 30년 이상 경력 보유한 글렌 체이페츠(Glenn Chafetz)를 모시고 '북한의 사이버 작전과 한미 안보 협력'을 주제로 논하였습니다.

자세한 인터뷰 내용을 첨부파일 참고 부탁드리겠습니다.

Received by NSD/FARA Registration Unit 10/30/2025 4:43:45 PM

KIPEC
KOREA INTER-PARLIAMENTARY EXCHANGE CENTER

KIPEC Focus: Expert Interview

North Korea's Cyber Operations and Their Impact on U.S.-South Korea Security Cooperation

KIPEC Focus: Expert Interview is a series that explores key developments in the United States through in-depth conversations with leading experts.

This report summarizes a conversation with Dr. Glenn Chafetz, Director of the 2430 Group, on North Korea's cyberstrategy and its implications for U.S.–South Korea security cooperation. The discussion was part of KIPEC's ongoing interview series designed to deepen understanding of emerging policy challenges relevant to both legislatures.

When most people think about North Korea, they picture nuclear tests or missile launches. Yet in recent years, cyber operations have become one of Pyongyang's most powerful and adaptable tools. Through cyber activities, North Korea has been able to generate foreign currency, steal technology and intelligence, and create disruption abroad, all at relatively low cost and risk.

To explore these issues, Dr. Chafetz, who brings more than 30 years of experience across government, academia, and the private sector, including service as a former CIA Chief of Station and the Agency's first Chief of Tradecraft and Operational Technology, shared his insights on how cyber operations support the regime's survival and influence.

The following Q&A captures key highlights from that discussion, offering an accessible overview of North Korea's cyber capabilities, the challenges of detection and deterrence, and the broader implications for U.S.–South Korea cooperation in the cybersecurity domain.

Q1. Why has cybersecurity become so central to North Korea's strategy?
Glenn: In short, crime pays. North Korea, like China and Russia, has learned that cyberattacks are profitable, hard to detect, and even harder to prevent. These operations weaken adversaries, steal valuable technology, and generate foreign currency, all of which are essential to keeping the Kim regime alive.

Received by NSD/FARA Registration Unit 10/30/2025 4:43:45 PM

Q2. What's one example that best illustrates North Korea's goals and capabilities?
Glenn: That's tough because there are many, but I'd point to what happened in February of this year when North Korea stole $1.5 billion from the crypto exchange ByBit. Considering North Korea's GDP is roughly $15 billion, that's enormous. Some estimates suggest they've stolen up to $6 billion in 2025 alone, and that's only what's been detected and reported.

Q3. Why is cryptocurrency theft such a key part of their strategy?
Glenn: Crypto is still the Wild West of finance. It's not impossible to trace, but it's much harder than tracking traditional dollar-based banking. It takes time, effort, and cooperation from exchanges, which gives thieves a head start. North Korea and other actors use "mixers" and layers of transfers to hide their tracks. If investigators can't move fast enough, the money is gone.

Q4. You've written about North Korean IT workers using fake or stolen identities to get remote jobs. How does that actually work?
Glenn: This one's fascinating and underappreciated. The FBI and others have put out public warnings, but we still underestimate the scale. One security officer told me there are two kinds of companies: those that know they've hired North Korean remote IT workers, and those that don't know it yet. These workers use fake or borrowed identities, forged addresses, and AI-altered video filters. They often refuse to appear on camera, claiming technical issues. And here's the kicker: they usually do solid work, so employers don't suspect a thing. It's not even a traditional "hack." It's really a human resources verification problem.

Q5. Why is this such a big issue for the U.S. and other countries?
Glenn: Because it's hidden in plain sight. Tens of thousands of these workers are operating remotely, especially in the U.S., and their salaries go straight back to the Kim regime.
Right now, governments treat companies that hire them as victims rather than as enablers, but that's a mistake. In export control law, if you knowingly send money or equipment to North Korea, you face penalties. Yet, if you indirectly fund the regime by hiring its IT workers, there's no consequence. That needs to change. We must realign the incentives.

Q6. Are there specific industries or countries that the regime tends to focus on?
Glenn: It's a pretty broad list: the U.S., South Korea, Japan, Taiwan, Bangladesh, Pakistan, the Philippines, and Cambodia—even smaller developing countries. They go where the defenses are weakest, and the payoff is highest. The 2016 Bangladesh Central Bank hack is a good example. They target anywhere with exploitable systems and lower oversight.

Q7. Why is it so hard for governments and companies to detect and stop these operations?
Glenn: A few reasons. First, these are mostly private sector targets. Our national security systems, especially in the U.S., were built to fight wars, not to protect private businesses from cyber theft. Agencies like the FBI have limited manpower compared to the scale of the problem. Second, private

Received by NSD/FARA Registration Unit 10/30/2025 4:43:45 PM

companies aren't built for counterespionage. Their focus is making cars, not spotting infiltration. And finally, the attacks are slow, diffuse, and incremental, not flashy or obvious. Combine that with poor incentives to report, and you've got a perfect storm.

Q8. How does North Korea compare to other countries like China or Russia in terms of capability?
Glenn: They're very good. Maybe not quite at China's or Russia's level, but close. People underestimate North Korea's technological sophistication. Their hackers and IT support staff are skilled, and that's one reason they succeed.

Q9. What more can governments do?
Glenn: Governments need to step up, devote more resources, share information across borders, and help the private sector defend itself. We spend billions preparing for hypothetical wars but ignore the war we're already in: A gray zone conflict fought online. We should also create incentives for companies to monitor, report, and strengthen their defenses instead of waiting for the government to fix it for them.

Q10. Turning to the alliance, how do Washington and Seoul currently work together on cybersecurity issues, and where do you see the most important opportunities to strengthen that cooperation going forward?
Glenn: I don't know the fine details, but clearly, it's not enough. North Korea, China, and Russia see themselves in conflict with both of our countries, and frankly, they're winning. We need deeper information sharing, coordinated defenses, and standardized policies. Hackers exploit gaps between jurisdictions; closing those gaps is key.

Q11. If you were speaking directly to lawmakers in South Korea, what would you say is the most important perspective they should keep in mind when shaping South Korea's cybersecurity and alliance strategy?
Glenn: Focus on the private sector. Our adversaries aren't firing artillery shells. They're stealing data, money, and technology from corporations. If governments don't help companies detect and report these attacks, they'll keep unknowingly funding Kim's nuclear and missile programs. Right now, there's a vicious cycle. Companies don't detect, so they think the problem is small. Since they think it's small, they don't invest in prevention, and that makes the problem even worse. We have to break that cycle by raising awareness, improving reporting, and incentivizing proactive defense.

Received by NSD/FARA Registration Unit 10/30/2025 4:43:45 PM

KIPEC
KOREA INTER-PARLIAMENTARY EXCHANGE CENTER

KIPEC 포커스: 전문가 대담

북한의 사이버 작전과 한미 안보 협력

KIPEC 포커스: 전문가 대담은 미국에서 발생하는 주요 사건에 대한 전문가를 인터뷰하면서 그 현안을 알아보는 시간입니다. 두번째 인터뷰로는 미국 현지시각 10월 30일 (목) 2430 그룹(2430 Group)의 설립자이자 전무이사인 글렌 체이페츠(Glenn Chafetz)를 모시고 '북한의 사이버 작전과 한미 안보 협력'을 주제로 논의했습니다.

체이페츠 박사는 정부, 학계, 민간 부문을 아우르는 30년 이상의 정보·안보 분야 경력을 보유하고 있으며, CIA(미 중앙정보국)에서 지부장(Chief of Station) 및 정보공작·작전기술 담당 수석 참모(Chief of Tradecraft and Operational Technology)로 근무한 바 있습니다. 체이페츠 박사는 이번 대담에서 북한의 사이버 작전이 정권의 생존, 외화 확보, 그리고 대외 영향력 확대를 위한 핵심 전략 도구로 어떻게 기능하는지를 분석하며, 이에 대응하기 위한 한미 양국의 협력 방향에 대해 심층적인 통찰을 제시했습니다.

대체로 국제사회에서 북한은 핵실험이나 미사일 발사로 대표되지만, 최근 들어 사이버 작전이 북한의 가장 비대칭적이면서도 전략적인 수단으로 부상하고 있습니다. 국제기구 및 미국 정부 기관의 최근 보고서에 따르면, 북한은 라자루스(Lazarus), APT38 등 국가 차원의 해킹 조직을 통해 수십억 달러 규모의 가상자산을 탈취하고, 이를 핵·미사일 프로그램과 정권 유지에 필요한 외화 조달 수단으로 활용하고 있습니다. 또한 이러한 사이버 활동은 기술·지식재산 탈취, 외국 금융망 침투, 사회기반시설 교란 등 다양한 형태로 전개되며, 적은 비용으로 높은 전략적 효과를 창출하는 비대칭적 수단으로 평가됩니다.

이러한 흐름 속에서, 체이페츠 박사는 북한의 사이버 작전이 실제로 어떻게 수행되고 있으며, 이를 억제하기 위한 국제적 대응은 어떠해야 하는지에 대해 심층적인 견해를 제시했습니다. 아래는 이번 대담의 주요 내용을 Q&A 형식으로 정리한 것입니다.

Q1. 왜 사이버 안보가 북한의 핵심 전략이 되었습니까?

답변: 간단히 말해, 범죄는 수익이 됩니다. 북한은 중국과 러시아처럼 사이버 공격이 수익성이 높고 탐지가 어렵다는 점을 배웠습니다. 이런 작전은 적대국의 역량을 약화시키고, 기술과 정보를 훔치며, 외화를 벌어들이는 등 김정은 정권의 생존에 필수적인 역할을 합니다.

Q2. 북한의 목표와 역량을 가장 잘 보여주는 사례는 무엇입니까?

답변: 한 가지만 고르기 어렵지만, 올해 2월 북한이 암호화폐 거래소 바이비트(ByBit)에서 약 15억 달러를 탈취한 사건을 꼽을 수 있습니다. 북한의 국내총생산(GDP)이 약 150억~250억 달러 수준으로 추정된다는 점을 고려하면, 이는 엄청난 규모입니다. 일부 추정에 따르면 2025년 한 해 동안만 약 60억 달러를 탈취한 것으로 보이며, 이는 확인된 사례만 집계한 수치입니다.

Received by NSD/FARA Registration Unit 10/30/2025 4:43:45 PM

Q3. 왜 암호화폐 절도가 북한의 전략에서 중요한 비중을 차지합니까?

답변: 암호화폐 시장은 여전히 금융의 '야생 서부'와 같습니다. 추적이 불가능한 것은 아니지만, 기존의 달러 기반 금융망보다 훨씬 어렵습니다. 거래소 간의 협조가 필요하고 시간이 걸리기 때문에, 범죄자들이 이를 악용해 먼저 자금을 이동시키는 경우가 많습니다. 북한과 다른 해커들은 믹서(mixer)나 다단계 송금을 활용해 자금의 출처를 숨깁니다. 수사기관이 그 속도를 따라잡지 못하면 돈은 이미 사라집니다.

Q4. 북한 IT 인력이 위조 또는 도용된 신원을 이용해 해외 기업에서 원격 근무를 한다고 하셨는데, 구체적으로 어떤 방식입니까?

답변: 매우 흥미로운 현상입니다. FBI를 비롯한 여러 기관이 경고를 내렸지만, 우리는 그 규모를 여전히 과소평가하고 있습니다. 한 대형 IT 기업의 보안 관계자는 이렇게 말했습니다. "북한 IT 인력을 고용한 기업은 두 종류뿐이다. 그 사실을 알고 있는 기업과, 아직 모르는 기업." 북한 IT 인력들은 도용된 신원이나 주소, 위조된 서류, AI로 조작된 영상 필터 등을 이용합니다. 화상 면접을 회피하거나 기술 문제를 핑계로 음성 통화만 요청하기도 합니다. 놀라운 점은, 이들이 실제로 업무를 성실하게 수행하기 때문에 의심을 사지 않는다는 것입니다. 이는 전통적인 '해킹'이 아니라, 인사 검증 시스템의 취약점을 이용한 사기 행위입니다.

Q5. 이러한 현상이 미국이나 다른 국가들에게 왜 큰 문제입니까?

답변: 겉으로는 보이지 않기 때문입니다. 수만 명의 북한 인력이 원격으로 일하며, 특히 미국 내에서 활동하고 있습니다. 이들의 급여는 결국 김정은 정권으로 송금됩니다. 현재 각국 정부는 이런 기업들을 '피해자'로 간주하지만, 사실상 '협력자'로 볼 여지도 있습니다. 수출통제법상, 북한에 자금이나 장비를 직접 보냈다면 처벌을 받습니다. 그러나 북한 IT 인력을 고용해 간접적으로 자금을 제공해도 제재는 없습니다. 이러한 정책적 인센티브 구조를 반드시 바꿔야 합니다.

Q6. 북한이 주로 노리는 산업이나 국가가 있습니까?

답변: 매우 다양합니다. 미국, 한국, 일본, 대만, 방글라데시, 파키스탄, 필리핀, 캄보디아 등 광범위한 지역이 대상입니다. 방어 체계가 약하고 수익 가능성이 높은 곳이면 어디든 공격합니다. 대표적인 사례가 2016년 방글라데시 중앙은행 해킹 사건입니다.[1] 규제가 느슨하거나 감독이 부족한 곳이 주요 표적이 됩니다.

Q7. 정부나 기업이 이러한 작전을 탐지하거나 차단하기 어려운 이유는 무엇입니까?

답변: 이유가 몇 가지 있습니다. 우선, 대부분의 공격 대상이 민간 부문입니다. 미국을 예로 들면, 국가 안보 체계는 본래 전쟁 수행을 위해 구축된 것이지 민간 기업의 사이버 범죄를 방어하기 위한 것이 아닙니다. FBI와 같은 기관은 인력과 자원이 제한적입니다. 또한 민간 기업은 대(對)스파이 방어 역량이 부족합니다. 기업의 전문성은 자동차를 만드는 것이지, 스파이를 찾아내는 것이 아닙니다. 게다가 북한의 공격은 지속적이고, 분산적이며, 점진적인 방식으로 이루어져 눈에 잘 띄지 않습니다. 여기에 신고 유인이 부족한 제도 환경이

---

[1] 2016년 방글라데시 중앙은행 해킹 사건은 해커들이 방글라데시 중앙은행의 뉴욕 연방준비은행 계좌에서 약 1억 100만 달러를 불법 송금한 대규모 사이버 공격입니다. 해커들은 은행 내부 시스템에 악성코드를 심고, 키로거(keylogger)를 통해 로그인 정보를 탈취했으며, 국제은행간통신협회(SWIFT) 금융망을 이용해 35건의 위조 송금 지시를 전송했습니다. 이후 돈의 대부분은 필리핀의 카지노를 거쳐 세탁되었습니다. 미국 연방 검찰 등 수사기관은 이 해킹이 북한 정부가 지원하는 라자루스 그룹(Lazarus Group)에 의해 수행되었다고 결론 내렸습니다.

Received by NSD/FARA Registration Unit 10/30/2025 4:43:45 PM

더해지면서, 문제는 점점 악화되고 있습니다.

Q8. 북한의 사이버 역량은 중국이나 러시아와 비교하면 어느 정도 수준입니까?
답변: 매우 높은 수준입니다. 중국이나 러시아만큼은 아니더라도 그에 근접한 수준입니다. 사람들은 흔히 북한을 기술적으로 낙후된 국가로 보지만, 이는 잘못된 인식입니다. 북한의 해커와 IT 지원 인력은 고도의 기술력과 숙련도를 보유하고 있으며, 이것이 이들이 성공하는 주요 이유입니다.

Q9. 각국 정부는 어떤 대응을 해야 한다고 보십니까?
답변: 정부는 더 많은 자원을 투입하고, 국경을 넘어 정보를 공유하며, 민간 부문이 스스로 방어할 수 있도록 지원해야 합니다. 우리는 막연한 미래의 전쟁에는 수십억 달러를 쓰면서, 이미 벌어지고 있는 '사이버 전쟁'에는 충분히 대응하지 않고 있습니다. 기업이 스스로 감시, 보고, 방어 체계를 강화하도록 제도적 유인책을 마련해야 합니다.

Q10. 한미 양국은 현재 사이버 안보 분야에서 어떻게 협력하고 있으며, 향후 어떤 부분을 강화해야 한다고 보십니까?
답변: 구체적인 세부 사항은 모르지만, 분명히 충분하지 않습니다. 북한, 중국, 러시아는 자신들이 이미 한미 양국과 사이버 전쟁 상태에 있다고 보고 있으며, 솔직히 말해 지금은 그들이 우위에 있습니다. 우리는 정보 공유 확대, 방어체계의 표준화, 정책 일치를 통해 대응해야 합니다. 해커들은 관할권의 빈틈을 파고듭니다. 그 틈을 줄이는 것이 핵심입니다.

Q11. 만약 한국 국회의원들에게 직접 조언을 한다면, 사이버 안보 및 한미 동맹 전략에서 가장 중요하게 고려해야 할 점은 무엇이라고 말씀하시겠습니까?
답변: 민간 부문에 주목해야 합니다. 적들은 포탄을 쏘지 않습니다. 그들은 기업의 데이터를 훔치고, 자금을 탈취하며, 기술을 빼갑니다. 정부가 기업이 이런 공격을 탐지하고 보고하도록 지원하지 않는다면, 기업들은 모르는 사이에 김정은 정권의 핵·미사일 프로그램을 재정적으로 지원하는 셈이 됩니다. 현재 악순환이 존재합니다. 기업은 공격을 탐지하지 못하니 문제를 작게 인식합니다. 문제를 작게 보니 예방에 투자하지 않고, 결과적으로 공격이 반복됩니다. 이 악순환을 끊기 위해서는 인식 제고, 보고 체계 강화, 예방적 방어 유인 제공이 필요합니다.

Received by NSD/FARA Registration Unit 10/30/2025 4:43:45 PM