Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

KIPEC
KOREA INTER-PARLIAMENTARY EXCHANGE CENTER

KIPEC Seminar Report

Changes in the International Cybersecurity Environment and the Future of U.S.-ROK Cyber Cooperation

Report on the Seminar Featuring James A. Lewis, Senior Adviser at the Center for Strategic and International Studies (CSIS)

The Korea Inter-Parliamentary Exchange Center (KIPEC) hosted a seminar on October 15, 2026 (local time), featuring James A. Lewis, Senior Adviser at the Center for Strategic and International Studies (CSIS), under the theme *"Defending the Digital Alliance: The Future of U.S.-ROK Cyber Cooperation."*

Mr. Lewis is a former U.S. Department of State diplomat and former member of the Senior Executive Service of the federal government. He is an expert in cybersecurity, technology policy, and international security. He also participated in cybersecurity negotiations of the United Nations Group of Governmental Experts (UN GGE), contributing to the development of norms for responsible state behavior in cyberspace.

The seminar examined how changes in the international order are affecting the cybersecurity environment and addressed the limitations of traditional cyber deterrence. Discussions focused on policy directions centered on resilience and active cyber defense. The seminar also explored the evolving nature of cyber threats resulting from the expansion of artificial intelligence (AI), ways to expand public-private information sharing and international cooperation, and the future direction of U.S.-ROK cyber cooperation, including policy challenges facing South Korea.

1. Changes in the International Order and the Cybersecurity Environment

Mr. Lewis emphasized that cybersecurity should be understood not merely as a technical issue, but within the broader context of changes in international politics and foreign policy. He explained that the recent increase in cyberattacks results from a combination of factors, including technological vulnerabilities, strategic competition among major powers, limitations in enforcing international norms, and the economic incentives driving cybercrime.

He observed that changes in the United States' international role and foreign policy priorities are contributing to a restructuring of the international order, with multiple major powers exercising influence. Nevertheless, he predicted that the importance of a stable international economic environment and cooperation among key partner countries would remain, given the growing interdependence among nations through international trade, global supply chains, and digital networks.

He also highlighted Asia's growing importance in the global economy and advanced technology industries. Citing the semiconductor industry as a prime example, he noted that Asian countries, including South Korea and Taiwan, play critical roles in global technology supply chains. Consequently, South Korea's strategic value and international influence have increased.

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

Meanwhile, he analyzed that cyberspace has become a major arena for strategic competition among nations. While the existence of nuclear weapons serves as a deterrent against direct military conflict among major powers, cyber activities can be conducted at relatively low cost and risk, making them an increasingly attractive instrument of interstate competition. In particular, cyber activities can cause information theft and economic damage even when they do not reach the threshold of a "use of force" under international law. Therefore, he pointed out that a response approach distinct from traditional military security measures is necessary.

Mr. Lewis assessed that the international community has made efforts to establish norms for responsible state behavior in cyberspace, but significant limitations remain in their practical implementation and enforcement. Drawing on his experience participating in UN GGE negotiations, he explained that reaching agreement on relevant norms in 2015 was an important achievement. However, subsequent increases in strategic competition among nations have made it more difficult to reach additional agreements.

Although discussions have continued through the United Nations Open-Ended Working Group (OEWG), he noted that international norms alone cannot sufficiently deter cyberattacks without meaningful accountability for violations. Accordingly, he emphasized that cybersecurity policy must extend beyond technical responses and be integrated with national security and foreign policy. Practical cooperation and response capabilities must also be strengthened alongside the continued development of international norms.

2. Limitations of Traditional Cyber Deterrence and New Policy Directions

Mr. Lewis assessed that traditional cybersecurity policies have relied substantially on deterrence and voluntary defense measures by the private sector. However, these approaches alone have proven insufficient to prevent persistent cyberattacks.

He explained that cyber deterrence cannot be expected to achieve the same effectiveness as nuclear deterrence because the costs and risks associated with cyberattacks are relatively low, while imposing meaningful accountability on perpetrators remains difficult. To address these limitations, cybersecurity policies are increasingly shifting toward strengthening resilience and active cyber defense.

Resilience refers to the ability to maintain essential functions and recover quickly even when an attack occurs, recognizing the reality that it is difficult to prevent every cyberattack in advance. Given the complexity of modern software and the existence of technological vulnerabilities, it is difficult to completely eliminate the possibility of network intrusions. Therefore, in addition to preventing intrusions, it is important to establish systems that can continuously provide essential services even after an attack has occurred.

He particularly emphasized the importance of resilience for critical infrastructure, such as electricity and water systems, because cyberattacks against these facilities can directly affect people's daily lives and the functioning of the nation. He noted that South Korea has a relatively well-developed legal framework for protecting critical infrastructure, but its operational

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

capabilities to maintain essential services and recover quickly during actual cyberattacks need further improvement.

Active cyber defense is an approach that goes beyond relying solely on investigations and punishment after an attack. It involves taking more proactive measures, such as disrupting cybercriminal activities or restricting attackers' operations. As a representative example, he cited tracing and recovering funds associated with cybercrime involving cryptocurrency. Since cryptocurrency transactions are often recorded on publicly accessible ledgers, law enforcement agencies can trace the movement of funds. If the incident is identified early and a prompt response is initiated, there may be opportunities to recover some of the stolen funds.

He also discussed measures to disrupt the operation of networks and infrastructure used in cybercrime. However, he explained that hacking directly into an attacker's network, commonly referred to as "hackback," can raise legal and diplomatic concerns. Therefore, the scope of permissible responses and the relevant legal authorities must be clearly defined before pursuing active cyber defense measures.

Mr. Lewis observed that South Korea has made progress in developing its cybersecurity policies over the past several years, but greater emphasis should now be placed on their practical implementation. In particular, he stressed the importance of translating policy directions concerning resilience and active cyber defense into concrete implementation frameworks.

3. The Expansion of Artificial Intelligence and Changes in Cyber Threats

Mr. Lewis predicted that advances in artificial intelligence would have a significant impact on the cybersecurity environment. However, he explained that the primary concern should not be that AI will necessarily create entirely new forms of threats, but rather that it will increase the speed and efficiency of existing cyberattacks.

He noted that AI can reduce the time and cost required to identify software vulnerabilities and develop attack programs that exploit them. Technology is advancing so rapidly that tasks that previously took several months may now be completed within days. He warned that cyber incidents could increase if defensive systems fail to keep pace with these developments.

Nevertheless, he emphasized that responding to these threats does not necessarily require building entirely new security systems. Implementing established basic security measures consistently, such as strong authentication systems, network segmentation, regular security patches, and vulnerability management, can provide substantial defensive benefits.

He identified the failure of many organizations to adequately implement these fundamental security measures as a major source of vulnerability. He stressed that, alongside discussions about the risks posed by AI technology itself, it is essential to improve the actual implementation of existing cybersecurity practices.

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

4. Institutional Challenges in Promoting Public-Private Information Sharing

Mr. Lewis emphasized that establishing an effective cybersecurity framework requires an institutional foundation that facilitates the sharing of threat information between government agencies and private companies.

He explained that companies may hesitate to share information about cyberattacks or security vulnerabilities with the government due to concerns about reputational damage, declining stock prices, competitive disadvantages, and potential legal liability. As a result, voluntary participation alone may not be sufficient to ensure effective information sharing.

He explained that, in the United States, institutional measures have been established to address these concerns. Under certain conditions, legal liability arising from the sharing of cyber threat information is limited, and safeguards have been introduced to prevent information sharing among companies from resulting in antitrust violations. However, he emphasized that these protections do not completely exempt companies from their cybersecurity management responsibilities.

Accordingly, he explained that it is important to strike an institutional balance that encourages companies to implement appropriate security measures while also facilitating prompt incident reporting and information sharing when cyber incidents occur. He noted that South Korea should also comprehensively review the scope of legal liability, safeguards for companies participating in information sharing, and relevant competition law provisions in order to improve the effectiveness of public-private information sharing.

5. Prospects for U.S.-ROK Cyber Cooperation and Policy Challenges for South Korea

Mr. Lewis predicted that security cooperation with South Korea would likely continue over the long term, even as U.S. foreign policy evolves. He assessed that South Korea remains an important partner for the United States because it is a longstanding ally, a key country in advanced technology industries such as semiconductors, and is strategically located in the Indo-Pacific region, which the United States considers a priority.

However, he emphasized that South Korea should maintain its existing cooperation with the United States while simultaneously expanding its cybersecurity partnerships with other countries. He identified Australia, the United Kingdom, Canada, and Japan as major potential partners. In particular, he noted that Australia has advanced cybersecurity capabilities and is actively interested in cooperation with South Korea. Canada and the United Kingdom were also identified as important countries with which South Korea could expand information sharing and joint response efforts.

He explained that South Korea's membership in Five Eyes, the intelligence-sharing alliance consisting of the United States, the United Kingdom, Canada, Australia, and New Zealand, would be difficult to achieve in practical terms. However, expanding bilateral cooperation with individual member countries would be a viable alternative. He also noted that strengthening

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

cybersecurity cooperation with Japan, as well as working with international organizations such as Interpol and countries within the Association of Southeast Asian Nations (ASEAN), could help enhance South Korea's cybersecurity capabilities.

Finally, he emphasized that the key to future cybersecurity cooperation lies in the ability to rapidly obtain information related to cyberattacks, share it with partner countries, and coordinate joint responses based on that information. To achieve this, he explained that it would be necessary to strengthen information-sharing systems based on mutual trust among partner countries and improve the relevant legal and institutional frameworks, including by granting law enforcement and intelligence agencies the necessary authorities to conduct investigations, share information, and respond to cyber threats.

KIPEC is registered under FARA. This material is distributed by the Korea Inter-Parliamentary Exchange Center (KIPEC) on behalf of the National Assembly of the Republic of Korea. Additional information is on file with the Department of Justice, Washington, D.C.

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

KIPEC
KOREA INTER-PARLIAMENTARY EXCHANGE CENTER

KIPEC 세미나 리포트

국제 사이버안보 환경의 변화와 한미 사이버 협력의 미래

부제 : 미국 전략국제문제연구소(CSIS) 제임스 루이스 선임고문 초청 세미나 결과 보고서

한미의회교류센터(KIPEC)는 2026 년 10 월 15 일(현지시간) 미국 전략국제문제연구소(Center for Strategic and International Studies, CSIS)의 제임스 루이스(James A. Lewis) 선임고문을 초청하여「디지털 동맹의 수호: 한미 사이버 협력의 미래(Defending the Digital Alliance: The Future of U.S.-ROK Cyber Cooperation)」를 주제로 세미나를 개최하였다.

루이스 선임고문은 미 국무부 외교관과 연방정부 고위공무원단(Senior Executive Service) 출신으로, 사이버안보와 기술정책, 국제안보 분야에서 활동해 온 전문가이다. 유엔 정부전문가그룹(UN Group of Governmental Experts, UN GGE)의 사이버안보 협상에도 참여하여 사이버 공간에서의 책임 있는 국가행동 규범 마련에 기여한 바 있다.

이번 세미나에서는 국제질서의 변화가 사이버안보 환경에 미치는 영향과 기존 사이버 억지력의 한계를 짚어보고, 복원력과 적극적 사이버 방어를 중심으로 한 정책 방향을 논의하였다. 아울러 인공지능(AI) 확산에 따른 사이버 위협의 변화, 민관 정보공유 및 국제협력 확대 방안을 중심으로 향후 한미 사이버 협력의 방향과 한국의 정책적 과제를 살펴보았다.

• 국제질서의 변화와 사이버안보 환경

루이스 선임고문은 사이버안보를 단순한 기술적 문제가 아니라 국제정치와 외교정책의 변화 속에서 이해해야 한다고 강조하였다. 최근 사이버 공격의 증가는 기술적 취약성뿐 아니라 주요 국가 간 전략적 경쟁, 국제규범의 집행 한계 및 사이버범죄의 경제적 유인 등이 복합적으로 작용한 결과라고 설명하였다.

그는 미국의 국제적 역할과 외교정책의 우선순위가 변화하면서 국제질서도 여러 주요 국가가 영향력을 행사하는 방향으로 재편되고 있다고 평가하였다. 다만 국제무역과 글로벌 공급망, 디지털 네트워크를 통한 국가 간 상호의존성이 심화되고 있어 안정적인 국제경제 환경과 주요 협력국 간 협력의 중요성은 유지될 것으로 전망하였다.

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

또한 세계 경제와 첨단기술 산업에서 아시아의 비중이 커지고 있다는 점에 주목하였다. 반도체 산업을 대표적인 사례로 들며 한국과 대만 등 아시아 국가들이 글로벌 기술 공급망에서 핵심적인 역할을 담당하고 있고, 이에 따라 한국의 전략적 가치와 국제적 영향력도 높아졌다고 평가하였다.

한편 사이버 공간은 국가 간 전략적 경쟁의 주요 영역으로 자리 잡고 있다고 분석하였다. 핵무기의 존재가 주요 국가 간 직접적인 군사충돌을 억제하는 요인으로 작용하는 반면, 사이버 활동은 상대적으로 낮은 비용과 위험으로 수행할 수 있어 국가 간 경쟁 수단으로 활용되고 있다는 것이다. 특히 국제법상 무력 사용(use of force)의 기준선에 이르지 않는 수준에서도 정보 탈취와 경제적 피해 등을 초래할 수 있다는 점에서 전통적인 군사안보와 구별되는 대응 방식이 필요하다고 지적하였다.

루이스 선임고문은 국제사회가 사이버 공간에서 책임 있는 국가행동 규범을 마련하기 위해 노력해 왔으나, 실질적인 이행과 집행에는 여전히 한계가 있다고 평가하였다. 유엔 정부전문가그룹(UN GGE)의 협상에 참여한 경험을 소개하면서, 2015 년 관련 규범에 합의한 것은 중요한 성과였지만 이후 국가 간 전략적 경쟁이 심화되면서 추가적인 합의를 도출하기 어려워졌다고 설명하였다.

유엔 개방형 실무그룹(Open-Ended Working Group, OEWG)에서도 관련 논의가 이어졌으나, 규범 위반에 대한 실질적인 책임 부과가 이루어지지 않는다면 국제규범만으로는 사이버 공격을 충분히 억제하기 어렵다고 지적하였다. 따라서 사이버안보 정책은 기술적 대응을 넘어 국가안보 및 외교정책과 연계되어야 하며, 국제규범의 발전과 함께 실질적인 협력 및 대응 역량을 강화할 필요가 있다고 강조하였다.

• 기존 사이버 억지력의 한계와 새로운 정책 방향

루이스 선임고문은 기존 사이버안보 정책이 억지력(deterrence)과 민간부문의 자율적인 방어에 상당 부분 의존해 왔으나, 이러한 방식만으로는 지속적인 사이버 공격을 막는 데 한계가 있었다고 평가하였다.

사이버 공간에서는 공격에 따른 비용과 위험이 상대적으로 낮고 실질적인 책임 부과도 어려워 핵 억지력과 같은 효과를 기대하기 어렵다는 것이다. 이러한 한계를 보완하기 위해

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

사이버안보 정책은 복원력(resilience)과 적극적 사이버 방어(active cyber defense)를 강화하는 방향으로 변화하고 있다고 설명하였다.

복원력이란 모든 사이버 공격을 사전에 차단하기 어렵다는 현실을 전제로, 공격이 발생하더라도 핵심 기능을 유지하고 신속하게 복구할 수 있는 능력을 의미한다. 현대 소프트웨어의 복잡성과 기술적 취약성을 고려하면 네트워크 침입 가능성을 완전히 배제하기 어려우므로, 침입 방지와 함께 공격 이후에도 필수 서비스를 지속적으로 제공할 수 있는 체계를 갖추는 것이 중요하다는 것이다.

특히 전력과 수도 등 중요 기반시설은 사이버 공격으로 인한 피해가 국민 생활과 국가 기능에 직접적인 영향을 미칠 수 있어 복원력 확보가 더욱 중요하다고 강조하였다. 한국은 중요 기반시설 보호를 위한 법적 체계를 비교적 잘 갖추고 있으나, 실제 공격 상황에서 필수 서비스를 유지하고 신속하게 복구할 수 있는 운영 역량은 더욱 강화할 필요가 있다고 언급하였다.

적극적 사이버 방어는 공격 발생 이후의 수사와 처벌에만 의존하지 않고, 사이버범죄 활동을 방해하거나 공격자의 활동을 제한하는 등 보다 능동적으로 대응하는 접근방식이다. 대표적인 사례로 암호화폐를 이용한 사이버범죄의 자금 추적과 회수를 제시하였다. 암호화폐 거래는 공개 거래원장을 기반으로 이루어지는 경우가 많아 수사기관이 자금 이동 경로를 추적할 수 있으며, 피해를 조기에 확인하고 신속하게 대응할 경우 탈취 자금의 일부를 회수할 가능성이 있다는 설명이다.

사이버범죄에 활용되는 네트워크와 기반시설의 운영을 방해하는 방안도 언급하였다. 다만 공격자의 네트워크에 직접 침입하는 해크백(hackback)은 법적·외교적 문제를 수반할 수 있으므로, 적극적 사이버 방어를 추진하려면 대응 범위와 법적 권한을 명확히 할 필요가 있다고 설명하였다.

루이스 선임고문은 한국이 최근 수년간 사이버안보 정책을 발전시켜 왔으나, 앞으로는 이를 실질적으로 이행하는 데 더 중점을 두어야 한다고 평가하였다. 특히 복원력과 적극적 사이버 방어를 위한 정책 방향을 구체적인 실행체계로 연결하는 것이 중요하다고 강조하였다.

- 인공지능 확산과 사이버 위협의 변화

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

루이스 선임고문은 인공지능의 발전이 사이버안보 환경에 상당한 영향을 미칠 것으로 전망하면서, 인공지능 자체가 완전히 새로운 형태의 위협을 만들어내기보다는 기존 사이버 공격의 속도와 효율성을 높이는 데 주목해야 한다고 설명하였다.

인공지능을 활용하면 소프트웨어 취약점을 신속하게 발견하고 이를 악용하는 공격 프로그램을 개발하는 데 필요한 시간과 비용을 줄일 수 있다는 것이다. 과거 수개월이 걸리던 작업이 며칠 만에 이루어질 수 있을 정도로 기술이 빠르게 발전하고 있으며, 방어체계의 개선 속도가 이를 따라가지 못할 경우 사이버 사고가 증가할 가능성이 있다고 전망하였다.

다만 이러한 위협에 대응하기 위해 반드시 완전히 새로운 보안체계를 구축해야 하는 것은 아니라고 강조하였다. 강력한 인증체계, 네트워크 분리, 정기적인 보안 패치 및 취약점 관리 등 기존에 권고되어 온 기본적인 보안조치를 충실히 이행하는 것만으로도 상당한 방어 효과를 확보할 수 있다는 것이다.

많은 조직이 이러한 기본적인 보안조치를 충분히 이행하지 않고 있다는 점을 주요 취약요인으로 지적하며, 인공지능 기술 자체의 위험성에 대한 논의와 함께 기존 보안체계의 실질적인 이행 수준을 높이는 것이 중요하다고 강조하였다.

• 민관 정보공유 활성화를 위한 제도적 과제

루이스 선임고문은 효과적인 사이버안보 체계를 구축하기 위해서는 정부와 민간기업 간 위협정보 공유를 활성화할 수 있는 제도적 기반이 중요하다고 강조하였다.

기업들은 사이버 공격이나 보안 취약점에 관한 정보를 정부와 공유할 경우 기업 이미지 훼손, 주가 하락, 경쟁상 불이익 및 법적 책임 등을 우려할 수 있어 자발적인 참여만으로는 충분한 정보공유가 이루어지기 어렵다고 설명하였다.

미국의 경우 이러한 문제를 완화하기 위해 일정한 요건 아래 사이버 위협정보 공유에 따른 법적 책임을 제한하고, 기업 간 정보공유가 반독점법 위반 문제로 이어지지 않도록 하는 제도적 장치를 마련해 왔다고 설명하였다. 다만 이러한 보호조치가 기업의 보안관리 책임을 전면적으로 면제하는 것은 아니라고 강조하였다.

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

따라서 기업의 적절한 보안조치 이행을 유도하면서도 사고 발생 시 신속한 신고와 정보공유가 이루어질 수 있도록 제도적 균형을 확보하는 것이 중요하다고 설명하였다. 한국 역시 민관 정보공유의 실효성을 높이기 위해 법적 책임의 범위, 정보공유 참여기업에 대한 보호장치 및 경쟁법 관련 규정 등을 종합적으로 검토할 필요가 있다고 언급하였다.

• 한미 사이버 협력의 전망과 한국의 정책적 과제

루이스 선임고문은 미국의 외교정책이 변화하더라도 한국과의 안보협력은 장기적으로 유지될 가능성이 높다고 전망하였다. 한국은 미국의 오랜 동맹국이자 반도체를 비롯한 첨단기술 산업의 핵심 국가이며, 미국이 전략적으로 중시하는 인도·태평양 지역에 위치하고 있다는 점에서 중요한 협력국이라고 평가하였다.

다만 한국은 미국과의 기존 협력을 유지하는 동시에 다른 국가들과의 사이버안보 협력도 확대할 필요가 있다고 강조하였다. 주요 협력 대상으로 호주, 영국, 캐나다 및 일본을 언급하였으며, 특히 호주는 높은 수준의 사이버안보 역량을 보유하고 한국과의 협력에도 적극적이라고 평가하였다. 캐나다와 영국 역시 정보공유 및 공동 대응 협력을 확대할 수 있는 주요 국가로 제시하였다.

미국, 영국, 캐나다, 호주, 뉴질랜드로 구성된 정보공유 협력체계인 파이브 아이즈(Five Eyes)에 한국이 가입하는 것은 현실적으로 쉽지 않지만, 개별 회원국과의 양자협력을 확대하는 것은 가능한 대안이라고 설명하였다. 또한 일본과의 사이버안보 협력 강화 및 인터폴(Interpol)을 비롯한 국제협력기구와 아세안(ASEAN) 국가들과의 협력도 한국의 사이버안보 역량을 강화하는 데 도움이 될 수 있다고 언급하였다.

끝으로 향후 사이버안보 협력의 핵심은 공격 관련 정보를 신속하게 확보하여 협력국과 공유하고, 이를 바탕으로 공동 대응하는 능력에 있다고 강조하였다. 이를 위해 협력국 간 신뢰를 바탕으로 정보공유 체계를 강화하고, 수사기관과 정보기관에 필요한 조사·정보공유·대응 권한을 부여하는 등 관련 법적·제도적 기반을 정비할 필요가 있다고 설명하였다.

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

KIPEC
KOREA INTER-PARLIAMENTARY EXCHANGE CENTER

KIPEC is registered under FARA. This material is distributed by the Korea Inter-Parliamentary Exchange Center (KIPEC) on behalf of the National Assembly of the Republic of Korea. Additional information is on file with the Department of Justice, Washington, D.C.

Received by NSD/FARA Registration Unit 11/06/2026 11:28:25 AM

Received by NSD/FARA Registration Unit 11/06/2026 11:28:27 AM

November 6 / KIPEC website / KIPEC seminar report

https://kipec.org/bsr/board.php?bo_table=archive&wr_id=34

https://kipec.org/ko/bsr/board.php?bo_table=archive&wr_id=34

Received by NSD/FARA Registration Unit 11/06/2026 11:28:27 AM