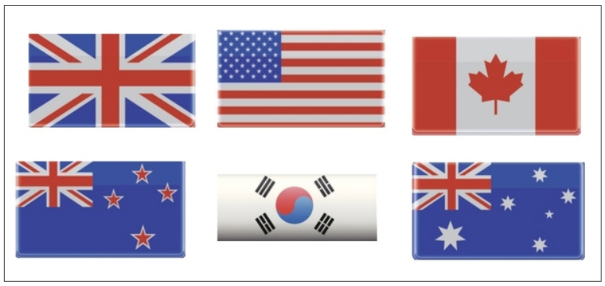
[한국사이버안보학회 칼럼] 파이브 아이즈 사이버 안보 국제전략과 한국 과제

입력 : 2024-10-02 14:01

사이버 안보 국제협력 진두지휘 주체 불분명...외교부 역할과 기능 명확하지 않아
국가 협력 강화 위해 사이버 안보 국제전략에서 외교부의 위치와 역할 되짚어봐야

[보안뉴스= 신승휴 서울대 정치외교학부 박사과정] 기술지정학(techno-geopolitics) 시대가 도래하면서 사이버 안보에 대한 국가적 접근도 변화를 거듭하고 있다. 오늘날 사이버 안보 전략, 좀 더 정확하게 '사이버 안보 국제전략'은 범정부 차원에서 거시적 목표를 설정하고 이를 추구하는 과정에 다양한 정부부처와 기관을 국제협력의 주체로 참여시킨다는 점에서 '국가책략(statecraft)'의 성격을 가진다. 이는 사이버 안보가 범분야 기술 문제(cross-cutting technical issue)이자 체제 수준의 도전이 됨에 따라 특정 기관 차원의 대응과 협력만으로는 더는 효과적으로 대응하기 어려워졌기 때문이다.



[이미지=gettyimagesbank]

국가책략의 관점에서 사이버 안보 국제전략을 수립·추진하고 있는 대표적 예는 다름 아닌 파이브 아이즈(Five Eyes) 국가들이다. 최근 미국, 영국, 캐나다, 호주, 뉴질랜드 등 파이브 아이즈 5개국은 민주주의 동맹을 통해 사이버 위협과 기술지정학적 위기에 공동대응하고자 하는 공유된 이해관계를 바탕으로 사이버 안보 국제전략을 추진하고 있다.

그 가운데 5개국의 전략은 이전보다 한층 더 △'네트워크화(networked)된 추진체계'를 채택하는 경향을 보이고 있다. 네트워크화된 추진체계는 여러 정부부처와 기관이 각기 담당하는 영역에서 개별적으로 사이버보안 체계를 구축하도록 허용함과 동시에 범정부 차원의 컨트롤타워를 수립해 사이버 안보에 대한 국가적 대응을 주도하게끔 하는 일종의 '복합형 모델'이다.

물론 5개국의 전략 추진체계는 △'컨트롤타워의 위치'의 측면에서 다소 차이를 드러낸다. 먼저 미국의 경우 대통령실 산하의 국가사이버실(ONCD)이 전략목표를 설정하고 부처별 대응을 조정하는 컨트롤타워 역할을 담당하지만, 동시에 국무부와 국토안보부의 역할과 권한도 매우 크다.

영국은 내각부를 통해 사이버 안보에 대한 국가전략을 수립하고 실질적인 전략의 수행은 정부통신본부(GCHQ)에 위임한다. 캐나다의 경우 과거 공공안전부에 있던 컨트롤타워의 기능이 현재는 통신보안국(CSE)으로 이전된 상태다. 호주는 총리내각부를 대신하여 내무부가 사실상 컨트롤타워의 역할을 수행하며 가장 큰 영향력을 행사하는 주체로 활동하고 있다. 뉴질랜드의 경우 정부통신보안국(GCSB)의 역할이 두드러지지만, 여전히 총리내각부가 컨트롤타워 역할을 수행하는 추진체계를 채택하고 있다.

한편, 5개국의 전략은 사이버 안보를 위한 국제협력에 있어 다양한 정부부처와 기관을 참여시킨다는 점에서 서로 비슷하지만, △'국제전략의 추진주체'가 누구인가에 따라 역시 크고 작은 차이를 가진다. 미국과 영국, 그리고 호주는 각각 국무부, 외무·영연방·개발부, 외교통상부가 사이버 안보 국제전략의 중심축이 되어 대외적 협력을 주도해오고 있다. 이들 국가에서는 사이버 안보에 특화된 정보기관의 대외부문 활동도 두드러지지만, 여전히 국제협력의 구체적인 분야를 설정하고 다자협의체에서 자국 정부를 대변해 전략적 이해관계를 전달하는 주체는 외교 전담 부처다.

캐나다와 뉴질랜드의 경우에도 역시 대외협력 모색은 각각 외교부와 외교통상부가 담당하지만, 동맹 차원의 협력을 뒤늦게 강화하기 시작한 만큼 미국, 영국, 호주와 비교할 때 외교 전담 부처의 활동은 다소 제한적으로 나타난다. 오히려 현 시점에는 정보기관이 국제전략의 핵심 주체로 기능하는 양상을 보인다.

다만, 이와 같은 차이에도 불구하고 5개국의 사이버 안보 국제전략은 다음의 공통된 특징적 현상을 보이며 점차 유사성을 더해가고 있다. 이는 전략 추진체계상 △대내적 치안 부문을 담당하는 정부부처의 대외적 활동이 증가하고 △외교 전담 부처의 기술안보 분야 역할이 강화되며 △정보기관의 국제적 공조 기능이 대폭 확장되는 것이다. 즉 사이버 안보에 대한 이들 국가의 전략이 국가책략의 관점에서 공공안전, 외교안보, 정보, 경제 등 다양한 영역의 경계를 넘나들며 국제협력을 모색하게 되면서 과거 특정 분야나 기능에 묶여있던 정부부처나 기관의 역할이 더욱 확장된 것으로 해석해볼 수 있다. 사이버 위협과 기술지정학적 위기에 대한 동맹 차원의 국제협력이 더욱 중요해질수록 파이브 아이즈 국가 간 전략 추진체계의 유사성은 갈수록 더 높아질 것이다.

그렇다면 우리의 상황은 어떠한가? 파이브 아이즈 국가들

가장 많이 본 기사 [주간]
1 [2024 영상보안 SoC & 모듈 리포트] 국가
2 전자상거래 강자 '네이버페이', 8월 피싱 사이
3 [2024 생체인증 리포트] 얼굴부터 손끝까지
4 [2024 XDR 리포트] 인력 부족과 넘치는 보
5 2024 국정감사, 보안·ICT·안전 분야 이슈 총...
6 가장 큰 골칫거리 문서형 악성코드, 이제는 '인
7 군 기밀 해킹 시도... 최근 5년간 월평균 1,0...
8 2024 국정감사, 보안·ICT·안전 분야 이슈 총...
9 2024 국정감사, 보안·ICT·안전 분야 이슈 총...
10 북한, 불법 사이버 활동으로 탈취한 자금
주요 기업별 기사

취약점 경고 및 보안 업데이트
• [2024-10-06] 지난해 1년간 불법 스팸문자
• [2024-10-06] 올해 국가유산청 및 소속기관
• [2024-10-06] 北 김수키, 독일 방산업체 '...
• [2024-10-06] '불법 복제' 만연... 최근...
• [2024-10-05] 北 김수키 해커그룹, '블루샤...
보안 · IT산업 동향
• 쿼리파이, 아시아 최대 보안 행사 ISEC ...
• 티피링크, 유기동물 보호 위해 Tapo 홈캠...
• 유니뷰, 북서울장애인보호작업시설에 CCTV ...
• 플랜티엠, 디지털 매거진 앱 모아진 갤럭시 ...
• 이지서티 김동례 대표, 행안부 디지털 행정서...

과 마찬가지로 한국도 '자유민주주의 수호를 위한 국제사회 협력 강화'를 목표로 삼아 동맹 중심의 국제협력을 꾸준히 모색해오고 있다. 추진체계 측면에서도 국가안보실과 국가정보원이 각각 컨트롤타워와 실무 주관기관이 되어 여러 정부조직의 대응을 통합·총괄하는 복합형 추진체계를 채택하고 있다. 그 가운데 국가정보원, 외교부, 과학기술정보통신부, 국방부 등 다양한 정부부처와 기관이 국제협력에 참여해오고 있다.

▲서울대 신승휴 정치외교학부 박사과정[사진=사이버안보학회]

그러나 사이버 안보 국제협력을 진두지휘하는 주체는 불분명하다. 특히 외교부의 역할과 기능이 명확하지 않다. '2022 국가사이버안보 기본계획'상 외교부는 '외교분야' 과제 수행을 담당하는 기관으로 나타날 뿐이다. 사이버 안보와 디지털 기술 분야 국제협력과 관련한 외교부의 역할이 파이브 아이즈 5개국의 외교 전담 부처와 비교할 때 그와 상응할 만큼 크고 중요한지 자신 있게 답하기 어렵다. 이들 국가와의 협력을 더욱 강화하기 위해서라도 사이버 안보 국제전략에서 외교부의 위치와 역할을 되짚어볼 필요가 있다.

[글_신승휴 서울대 정치외교학부 박사과정]

김경애기자 기사보기

1 0

연관 뉴스

- [한국사이버안보학회 칼럼] AI·사이버 외교의 현황과 쟁점

헤드라인 뉴스

- 아시아 최대 규모 보안 콘퍼런스 ISEC 2024, 16~17일 양일간 논의되는 주요 이슈...
- 北 김수키, 독일 방산업체 '딜 디펜스' 해킹... K-방산에 미치는 영향과 파장은?
- 北 김수키 해커그룹, '블루샤크' 전술로 APT 공격 감행
- [한 주를 관통하는 보안 소식] 2024년 10월 1주차, 'New Order'
- [영화&보안] 숨겨진 축복에 관한 숨겨진 이야기, '그녀에게'

TOP 뉴스

- [ISEC 2024 미리보기] Tenable, ...
- [ISEC 2024 미리보기] 크로니아이티, 보...
- [ISEC 2024 미리보기] 쿼리시스템즈, S...
- [ISEC 2024 미리보기] 쿼드마이너, 보안...
- 지난해 1년간 불법 스팸문자 무려 3억건... ...
- 올해 국가유산청 및 소속기관 해킹시도 6,233...
- KITRI, '2024 제16회 사이버 영토 수...
- [2024 생체인증 리포트] 엄굴부터 손끝까지 ...

로그인 후 댓글을 입력하세요.
확인

조회순 추천순 스크랩순

1  북한, 불법 사이버 활동으로 탈취한 자금 2...

2  北 김수키 해커그룹, '블루샤크' 전술로 A...

3  [한 주를 관통하는 보안 소식] 2024년 ...

4  [영화&보안] 숨겨진 축복에 관한 숨겨진 이...

5  KAIST 사이버보안연구센터, 'Gamble...

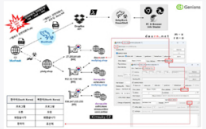
설문조사

최근 발생한 크라우드 스트라이크의 보안 SW 업데이트 오류 사태처럼 SW 공급망에 보안이슈가 발생할 경우 관련된 각종 시스템 및 IT 인프라 마비가 일어날 수 있다는 게 드러났습니다. 이러한 공급망 보안을 위협하는 가장 큰 요인은 무엇이라고 생각하시나요?

- 랜섬웨어, 피싱 등의 사이버 공격
- SW 업데이트 및 SW 교체 과정에서의 오류
- SW 자체에 존재하는 보안 취약점

아시아 최대 규모 보안 콘퍼런스 ISEC 2024, 1...


北 김수키, 독일 방산업체 '딜 디펜스' 해킹... K...


北 김수키 해커그룹, '블루샤크' 전술로 APT 공격 ...


[한 주를 관통하는 보안 소식] 2024년 10월 1주...


[영화&보안] 숨겨진 축복에 관한 숨겨진 이야기, '그...

북한, 불법 사이버 활동으로 탈취한 자금 2023년에만...


2024 국정감사, 보안·ICT·안전 분야 이슈 총정리...

[bnTV] 증권가가 주목한 이 기업, 준비된 밸류업 ...