북한개발소식

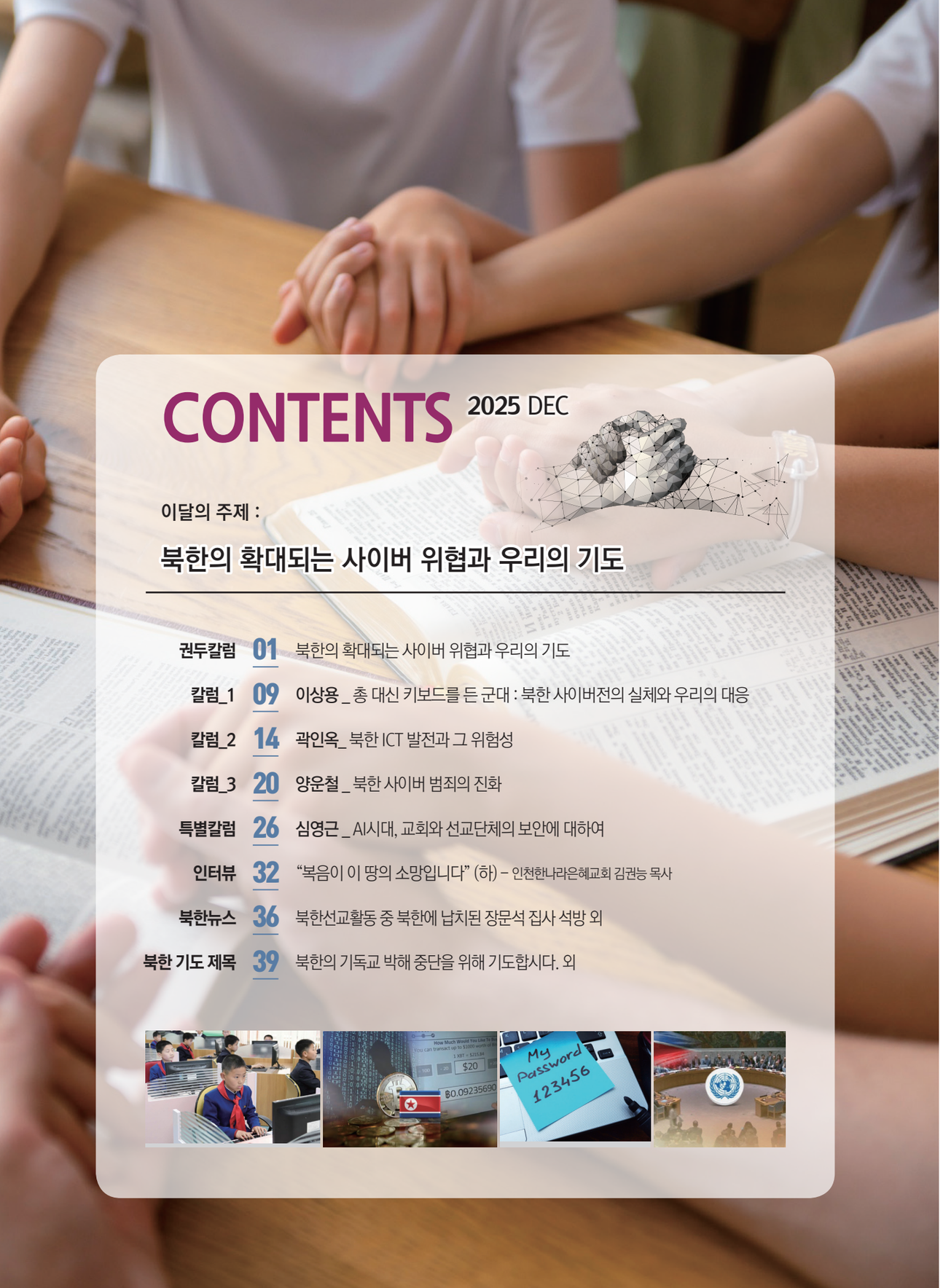
2025 DEC
12
통권 242호

이달의 주제
북한의 확대되는
사이버 위협과 우리의 기도

특집 칼럼
AI시대, 교회와 선교단체의
보안에 대하여

북한뉴스
북한선교활동 중 북한에 납치된
장문석 집사 석방 외

한국 오픈도어 북한선교연구소
전세계 박해받는 교회를 섬기는 오픈도어선교회



CONTENTS 2025 DEC

이달의 주제 :

북한의 확대되는 사이버 위협과 우리의 기도

권두칼럼

북한의 확대되는 사이버 위협과 우리의 기도

오픈도어선교회 북한선교연구소

북한이 세계적인 해킹 강국이라는 사실은 이제는 새삼스럽지 않다. 미국의 FBI 같은 주요 정보기관과 IT 보안 관련 기업들은 북한의 해킹 능력을 세계 3위권으로 평가하고 북한의 공격을 지속적으로 경고하고 있다.[1] 그만큼 북한의 사이버 공격은 그 빈도나 수준에서 세계적인 수준에 도달해 있다.

이러한 북한의 사이버 공격 표적이 일반 교회로까지 확대되고 있다. 올 6월 한 대형 교회에서는 새벽예배를 유튜브로 생중계하던 중 북한 인공기와 북한 국가가 송출되는 사고가 발생했다.[2] 이와 관련하여 해당 교회 측은 같은 시간대에 다른 교회도 새벽예배가 해킹되는 동일한 사건이 발생한 것을 확인했다며 외부의 해킹이 분명하다고 언급했다.[3] 비슷한 시기에 보안업체 지니언스는 교회를 대상으로 북한 해커들의 공격 시도에 대해 보고했다. 보고서에 따르면 북한 해킹조직 김수키는 ‘트랜지셔널 저스티스 미션(Transitional Justice Mission)’이라는 이름의 페이스북 계정을 개설하고, 자신을 교회 전도사 또는 연구원 신분의 목사로 소개하며 대북 분야 종사자들과 접촉을 시도했다. 이들은 대북 분야에 종사하는 목회자 다수에게 친구 신청 및 메신저로 접근한 뒤 대북 선교 자료를 공유한다면서 상대방에게 해당 악성파일을 전송받도록 유도하는 수법을 쓴 것으로 밝혀졌다.[4]

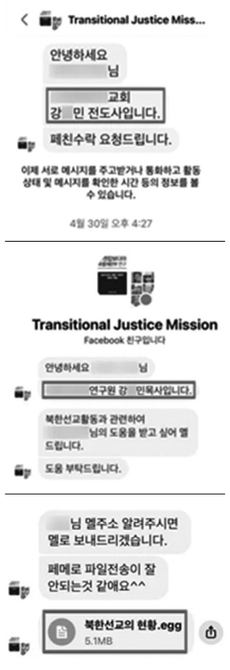
---

1) 北 해킹능력 세계 3위… “한국 국가시스템 순식간에 무력화 가능”, 조선닷컴, (2022.01.22) 〈https://www.chosun.com/politics/north_korea/2022/01/22/JOMOPWOATNEPZDVA45KXMJBBOM/〉

2) 온누리교회 유튜브 새벽예배 중 북한 영상 송출…해킹 의심에 보안 강화 나서, 보안뉴스 (2025.06.19.), 〈https://www.boannews.com/media/view.asp?idx=137733〉

3) 이재훈 목사, 유튜브 北 인공기 해킹 사고에 “외부 소행 분명”, 크리스천투데이(2025.06.22), 〈https://www.christiantoday.co.kr/news/368969〉

4) "북한선교 도와주세요"…전도사·목사 사칭한 北 해커 '주의', 데일리굿뉴스(2025.06.11.),〈https://www.goodnews1.com/news/articleView.html?idxno=448431〉



〈전도사·목사를 사칭해 북한 선교 종사자들에게 SNS 기반 해킹을 시도하는 북한 해커 (자료=지니언스)〉

그동안 선교 현장에서는 북한의 해킹에 따른 위협에 대한 경고의 목소리가 있어 왔다. 북한 관련 사역 단체나 활동가들을 대상으로 한 이메일 해킹 시도나 테러 활동들이 상당한 빈도로 있었다. 그렇지만 이제는 이러한 위협이 일선 교회에까지 미치게 되면서 꼭 북한 관련 활동을 하지 않는 교회라 하더라도 북한의 사이버 위협에 대해 알고 대비해야 하는 상황이 전개되고 있다. 이 글에서는 북한의 사이버 위협 실태에 관하여 살펴보고 교회와 선교 현장에 주는 시사점 등에 관하여 생각해 보고자 한다.

북한의 사이버 공격 역량과 조직

IT 기반이 부족한 북한이 어떻게 현재의 광범위한 사이버 공격을 수행할 수 있을까? 이는 북한이 수십 년 전부터 해당 분야 인재 양성에 힘써왔기 때문이다. 북한은 2000년부터 만경대학생소년궁전, 평양학생소년궁전, 금성학원, 금성제1중학교에 컴퓨터 수재들을 전문적으로 키워내는 컴퓨터 수재반을 마련하고 중등교육 단계에서부터 본격적인 컴퓨터 수재 교육을 진행해왔다.[5] 이렇게 양성된 전문 인력의 규모는 이미 수만에 육박한다. Dean J. Ouellette(2021)는 2019년 기준으로 북한 대학의 관련 학과 졸업자 및 학위자 배출 규모, 그 외 관련 행사 참여 규모 등을 바탕으로 북한의 IT 인력을 10만여 명으로 추산하였다.[6] 세계 80여 개국에서 1-3만여 명의 대학생이 참여하는 국제 프로그래밍 경연대회 '코드쉐프'에서 북한 학생들이 수년간 최상위권 성적을 거두는 등[7] 교육 수준이나 실력도 뛰어난 것으로 알려졌다. 이렇게 양성된 인력 중 상당수는 사이버전에 투입된다. 우리 군 당국은 북한의 사이버전 인력 규모를 약 6,800여 명으로 추산하고 있다.[8]

이렇게 준비된 인력을 바탕으로 북한은 다양한 해킹 그룹을 운영하고 있다. 북한 해킹조직은 대부분 북한군의 '정찰총국' 산하 기술정찰국(3국) 소속으로 알려져 있다. 2009년 출범한 정찰총국은 인민부력부 정찰국, 노동당 작전부, 중앙당 35호실 등에 분산되어 있던 공작 부서를 통합한 해외·대남 정보기구이다. 정찰총국이 출범하면서 산하 사이버전 조직도 확대 개편되었고, 북한의 사이버 공격 활동이 본격화되었다.[9]

우리가 뉴스 보도를 통해 접하게 되는 북한의 해킹 조직은 혼란스러울 정도로 다양한데, 이는 각 해킹조직이 알려진 정식 명칭이 있는 것이 아니라 탐지한 보안업체들이 부여한 명칭에 따라 각각 불리기 때문이다. 그러다 보니 같은 조직이지만 다른 이름으로 불리는 경우도 있다. 이를 정리해서 보면 북한의 해킹집단은 크게 4그룹으로 나뉘는데, 각각 라자루스(Lazarus) 그룹, 김수키(Kimsuky) 그룹, APT37 또는 금성121 그룹, APT38 그룹이다.[10] 각 그룹은 공격 대상과 목적이 조금씩 다르다. 라자루스와 APT38이 사이버범죄 수익에 집중한다면, APT37과 김수키는 정보 탈취에 특화된 전형적인 국가 지원 해킹 행태를 보인다. 이 중 라자루스는 초창기에는 정보 탈취·사이버 테러에 중점을 두었으나, 현재는 금융기관과 암호화폐 거래소 등을 공략하는 모습을 보인다.[11] 이 외에 통일전선부나 국가보위성도 해킹에 관여한다는 주장도 있다.[12]

〈표, 북한의 해킹집단[13]〉

해킹집단	공격 대상	목적	기타 명칭
라자루스 (Lazarus)	- 전 세계 금융기관 - 공공기관, 군, 기업	정보 탈취 법죄수익 사이버 테러	히든 코브라×(Hidden Cober) - 안다리엘* (Andariel)
APT37	- 한국 + - 공공기관 및 개인	정보 탈취	리버(Reaper) 스카크러프트(Scarcruft)
APT38	- 전 세계 금융기관 - 카지노	범쇠수익	블루노로프(Bluenorope) 템프 허밋(TEMP. Hermit) 비글보이즈×(BeagleBoys)
김수키 (Kimsuky)	-한국 + - 공공기관 및 개인 (한국수력원자력 등)	정보 탈취 사이버 테러	벨벳 천리마(Velvet Chollima) 탈륨(Thallium)

주 : 1) + 한국 및 미국, 일본, 중국 등 주요 국가
2) × 미 정부가 사용하는 명칭
3) * 라자루스 하위그룹

북한발 사이버 공격은 그 공격 자체로도 심각한 피해를 유발하지만, 이로 인한 파급 효과가 더욱 큰 문제가 되고 있다. 북한의 사이버 공격이 대북 제재를 우회

5) 북한 2000년부터 국가적 차원 IT영재 교육, NK경제, (2019.05.01.), 〈http://www.nkeconomy.com/news/articleView.html?idxno=1375〉
6) Dean J. Ouellette (2021), 북한의 ICT 산업 인력 관련 법정책, 사회법연구, 45, 369-414.
7) 북한 김일성대, 국제 프로그래밍 경연서 7회연속 우승, 연합뉴스, (2022. 12. 31.), 〈https://www.yna.co.kr/view/AKR20221231026100504〉
8) 「2022 국방백서」, 서울:대한민국 국방부 (2022), 25.
9) 박찬영, 김현식 (2024), "북한의 사이버 공격 변화 양상에 대한 연구", The Journal of the Convergence on Culture Technology (JCCT), 10:4, p. 178.
10) 각 그룹명에서 APT는 지능형 지속 위협(Advanced Persistent Threat: APT)을 의미한다. 이는 해커가 특정 타깃을 선정한 후 소셜 엔지니어링 등 다양한 방법을 이용해 네트워크에 침입한 후 공격이 성공할 때까지(혹은 완전히 불가능해 지기 전까지) 짧게는 수 주, 길게는 수 년에 걸쳐 줄기차게 공격하는 방식을 말한다. (참고: 기획재정부 시사경제용어사전)
11) 고명현 (2021), "북한의 사이버 전력(戰力)과 금융범죄" KDI 북한경제리뷰 21년 10월호, 59-60.
12) "북한 정찰총국 외에 통일전선부, 국가보위성도 사이버 해킹 관여", VOA, (2022.03.24.) 〈https://www.voakorea.com/a/6498327.html〉
13) 고명현 (2021), 59.

하는 하나의 방법으로서 북한의 핵무기 개발과 직접적인 연관을 보이고 있기 때문이다. 23년 6월 바이든 행정부의 한 고위 관계자는 닛케이에 2018년 이후 북한의 공격이 핵 및 미사일 프로그램과 함께 급격히 증가했고, 암호화폐 탈취와 사이버 공격이 평양 정권의 주요 자금원이라는 점에 매우 우려하고 있다고 언급했다.[14] 2024년 유엔 안보리 산하 대북제재위원회는 대량살상무기 개발 프로그램 재원의 40%가 해킹, 사이버 공격 등 불법적인 사이버 수단으로 조달됐다고 회원국 보고를 토대로 지적하기도 했다.[15]

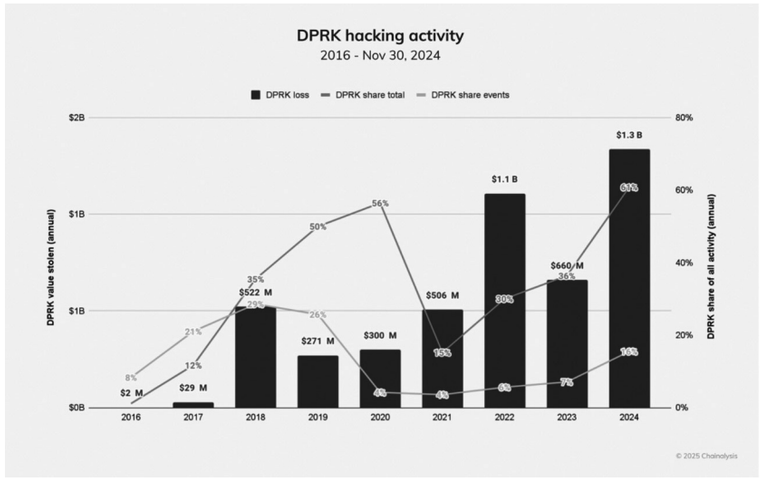
북한의 사이버 공격 추세

그렇다면 북한은 어떤 방식으로 사이버 공격을 벌이고 있을까? 최근 관찰되는 특징적인 북한의 사이버 공격 방식을 살펴보자. 먼저 프리랜서 개발자로 위장 취업하는 형태이다. IT업체에 원격근무 개발자로 취업한 후, 내부에서 악성코드나 랜섬웨어를 배포하며 공격하고 돈을 뜯어내는 방식이다. 글로벌 보안 기업 크라우드스트라이크는 북한 해커들이 지난해 320여 개 기업에 원격근무 소프트웨어 개발자로 위장 취업했고, 대규모의 내부자 공격 캠페인을 감행했다고 밝혔다.[16]

암호화폐 해킹 활동은 활발한 것을 넘어 최대 규모를 갱신하고 있다. 미국 블록체인 분석 기업 체이널리시스(Chainalysis)는 2025년 5월 발표한 보고서 전 세계에서 최소 409억 달러가 불법 암호화폐 주소로 흘러 들어간 것으로 나타났다. 2024년 기준, 북한은 총 47건의 암호화폐 해킹을 통해 13억 4000만달러를 탈취했다. 이는 전체 해킹 피해액의 61%에 해당한다.[17] 더 나아가 북한 해킹조직은 2025년 2월, 단일 사건으로는 역대 최대규모인 약 14억 6천만달러 상당의 자산을 탈취한 바이빗(Bybit) 거래소 해킹 사건을 비롯하여 올해에만 약 20억달러(한화 약 2조 7천억 원) 규모의 가상화폐를 탈취한 것으로 분석됐다. 이는 역대 최대 피해액이다.[18]

기존 시스템의 취약점을 활용한 공격 시도도 잇따르고 있다. 23년 4월 북한의 해킹그룹 '라자루스 Lazarus'가 인터넷 뱅킹 등에 쓰이는 금융보안인증 프로그램인 '이니세이프(INISAFE)'을 역이용하여 국내 61개 기관 207대의 PC를 해킹한 것으로 확인되었다.[19] 해당 사건은 1,000만 대 이상 설치된 것으로 추정되는 보안 프로그램을 통한 해킹이어서 더 충격적이었다. 2024년 5월에는 북한 해커 조직 '라자루스'가 국내 법원 전산망을 2년 넘게 해킹해 각종 개인 정보가 포함된 1,014GB 규모의 자료를 빼낸 사실이 정부 합동 조사로 드러났다.[20] 이 외에도 24년 1월 김수키 그룹은 국내 건설 분야 직능 협회 홈페이지를 통해 악성코드를 유포하여 홈페이지에 접속한 지자체, 공공 기관, 건설 기업 등의 업무 담당자 PC를 악성코드에 감염시켰고, 24년 4월에는 안다리엘 APT 그룹이 국내 정보 보안 SW의 취약점을 악용해 건설 및 기계 분야 업체에 원격 제어 악성코드를 침투시킨 사례도 확인되었다.[21]

〈북한의 암호화폐 해킹 활동 추이, (자료=Chianalys)〉



최근에는 북한의 해킹 기술이 사회공학적 기법[22]과 기술적 기법을 결합시켜 높은 성공률을 노리는 전략으로 발전하고 있다. 올 11월 북한 배후 해킹 조직이 안드로이드 스마트폰과 PC를 원격 조종해 주요 데이터를 통째로 삭제하는 사이버 공격을 한 정황이 처음 발견됐다. 지난 9월 5일 북한 해커는 국내 한 심리 상담사의 스마트폰을 초기화하고 탈취한 카카오톡 계정을 통해 '스트레스 해소 프로그램'으로 위장한 악성 파일을 지인들에게 보냈다. 같은 달 15일에도 한 북한 인권

14) "North Korea Makes 50% of Income from Cyber-Attacks: Report", Infosecurity Magazine (2023.06.05.), 〈https://www.infosecurity-magazine.com/news/north-korea-makes-50-income/〉

15) 유엔 "北, 사이버탈취 6년간 4조원대‥핵개발 재원의 40% 조달", MBC(2024.03.21.), 〈https://imnews.imbc.com/news/2024/world/article/6581968_36445.html〉

16) 북한 해커, AI로 가짜 이력서·위장취업…지난해 320곳 피해, 뉴스1(2025.09.01.), 〈https://www.news1.kr/it-science/general-it/5897843〉

17) "북한, 작년 코인 해킹으로 2조원 탈취 '역대 최대'" 암호화폐 범죄 수법도 진화, 블록미디어(2025.05.12.), 〈https://www.blockmedia.co.kr/archives/906106〉

18) 북한 라자루스 그룹, 2025년 가상화폐 2조7천억원 탈취…역대 최대 규모, 데일리시큐(2025.10.18), 〈https://www.dailysecu.com/news/articleView.html?idxno=201211〉

19) 1,000만 명 쓰는 보안인증 프로그램, 북한 해킹 조직에 뚫렸다, imbc, (2023.04.18.) 〈https://imnews.imbc.com/news/2023/society/article/6475153_36126.html〉

20) 北에 1TB 해킹당한 대법원, 뭐가 털렸는지도 모른다, 조선일보 (2024.05.13.), 〈https://www.chosun.com/national/2024/05/13/VFMMY3PYINEL7IKHG4KNRAHTH4/〉

21) 북한 해킹 그룹, 공급망 공격으로 국내 기업 노린다, 테크월드(2024.08.07.), 〈https://www.epnc.co.kr/news/articleView.html?idxno=305023〉

22) 사회공학적 해킹은 시스템이 아닌 사람의 취약점을 공략하여 원하는 정보를 얻는 공격기법이다. 인터넷의 발달로 이메일, 인터넷 메신저, 트위터 등을 통해 사람에게 접근하는 채널이 다각화됨에 따라 지인으로 가장하여 원하는 정보를 얻어내는 공격방법을 주로 뜻한다. (참고: 지식경제용어사전)

운동가의 안드로이드 스마트폰이 초기화되고, 탈취된 카카오톡 계정을 통해 지인 36명에게 악성 파일이 유포했다. 이 악성 파일은 피해자의 스마트폰, PC 등에 침투한 뒤 장기간 잠복하며 구글 및 국내 주요 정보기술(IT) 서비스 계정 정보 등을 탈취했다. 피해자들의 스마트폰, 태블릿, PC에서 사진과 문서, 연락처 등 주요 데이터를 삭제하기도 했다. 카카오톡 메시지를 통한 악성코드 유포는 신뢰가 있는 지인 관계를 위장한 전형적인 사회공학 기반이지만, 안드로이드 스마트기기 데이터 삭제와 계정 기반 공격 전파 등 여러 수법을 결합한 전략은 전례 없는 것으로서, 북한의 사이버 공격 전술이 사람들의 일상으로 파고드는 실질적 파괴 단계로 고도화되고 있음을 보여준다.[23]

이렇게 다양화되는 북한의 사이버 공격은 시기별로 당국의 정책적 필요에 따라 중점적인 공격 표적이 정해지는 모습을 보인다. 박찬영, 김형식(2024)은 북한의 공격을 시기/목적별로 1기에서 3기로 구분하였는데, 제1기는 2009년부터 2016년까지 주로 일어난 대남 도발 형태의 공격, 2기는 2016년부터 본격화한 외화벌이를 위한 금융기관 공격 및 암호화폐 탈취 등의 공격, 3기는 21년도부터 활발해지는 방산업체 기술 탈취 시도이다. 이러한 기수 구분은 북한 사이버전 국면의 전면적 전환을 의미하는 것은 아니며, 모든 시기에 걸쳐서 1~3기에 언급된 공격이 이루어지고 있다. 그렇지만 북한의 전략목표에 따라 시기별로 특별히 중점적으로 이루어지는 북한의 사이버 공격 대상이 있다는 것인데, 이런 맥락에서 최근 북한의 적극적인 기술탈취 활동은 2021년 8차 당대회에서 김정은 위원장이 제시한 전략무기 5대 과업 달성을 위한 것으로 분석했다.[24] 실제로 올해 한 컨퍼런스에서 국가사이버안보센터 담당관은 "북한은 방산의 '비읍(ㅂ)'만 들어가면 다 턴다"라고 표현하면서 "북한은 2021년 1월 당대회에서 '국방력 발전 5개년 계획'을 수립했고, 올해가 성과 마지막 해"라며 "올해는 북한의 미비 분야를 대상으로 방산 기술 절취에 들어갈 것으로 보인다"라고 언급하기도 했다.[25]

북한 사이버 위협에 대한 우려와 우리의 기도

북한의 사이버 위협은 외화벌이나 군사정보 탈취에만 국한되지 않는다. 북한은 직간접적으로 북한 선교 사역에 대한 사이버 위협을 가하고 있다. 그간 많은 북한 선교 및 인권 관련 활동가와 기관들이 북한으로부터 다양한 형태의 사이버 공격을 당해왔다. 북한 관련 사역 단체나 사역자의 이메일이 해킹을 당하는 경우는 이미 흔한 일이 되어버렸다. 2019년에는 북한의 해킹조직 '금성121'조직의 소행으로 보이는 북한선교학교 지원서 사칭 공격이 발견되기도 했다.[26] 앞서 소개한 바와 같이 북한 인권 활동가의 개인 스마트폰과 카카오톡 계정을 해킹한 사례나 탈북민 사역 참여를 위장하며 관련 사역자나 교회 등을 공격하는 사례, 더 나아가 일반 교회의 예배에 대한 해킹까지 보고되고 있다. 이 외에도 보고되지 않은 북한의 기독사역자 및 단체, 교회에 대한 사이버 공격 시도도 상당한 규모일 것으로 추정된다.

북한이 사역 단체와 교회를 대상으로 왜 이러한 사이버 위협을 가하는 것일까? 가장 먼저는 교회나 선교단체가 가진 정보에 대한 접근 및 탈취 목적을 꼽을 수 있다. 즉 북한에 대한 선교 활동을 방해하고 관련 사역자 정보를 얻어내려는 목적이다. 이와 함께 해킹을 통해 원활한 사역을 방해하고 더 나아가 공격받고 있다는 의식을 심어줌으로써 두려움을 유발하고 사역을 위축시키고자 하는 의도를 짐작해 볼 수 있다. 더 나아가 최근 관찰되는 북한 선교와 특별한 연관성이 없는 일반 성도나 교회를 향한 공격은 북한이 가진 기독교와 한국 교회를 향한 적대감에 의한, 사역을 방해하고자 하는 목적에 따른 것으로 볼 수 있다.

교회나 기독교 관련 기관과 단체가 일반적인 해킹 공격의 대상이 되는 일은 종종 있지만, 이는 기업체에 비해 상대적으로 취약한 보안 시스템을 악용하여 돈을 목적으로 한 공격이 보통이다.[27] 하지만 북한의 공격은 이보다는 악성 코드를 통해 관련 사역자 및 선교 기관과 교회에 피해를 주고 정보를 탈취하려는 모습이 주로 관찰된다. 특히 단순히 악성코드를 심은 이메일을 무차별적으로 살포하는 것이 아니라, 특정 교회의 목사나 전도사로 속여 접근하고 각종 SNS를 이용해 신뢰를 쌓은 뒤, '긴급 기도 요청', '교회 행사 안내', '탈북민 돕기 후원 요청'과 같이 신자라면 무심코 지나치기 어려운 내용으로 위장한 메시지를 보내는 모습은, 이들이 한국교회의 문화에 대해 정통해 있고 이들의 공격 방식이 오랜 기간을 거쳐 발전된 것임을 보여준다. 앞서 살펴본 바와 같이 북한의 해킹 활동이 북한 당국의 정책이나 필요, 중점 사항에 크게 좌우되고 있음을 고려한다면, 북한 당국이 북한 선교에 참여하는 개인이나 단체를 넘어 한국 교회를 전략적으로 사이버 공격의

23) 北해킹조직, 스마트폰·PC·카톡 장악…사이버 공격 정황 첫 발견, 중앙일보(2025.11.10), 〈https://www.joongang.co.kr/article/25380784〉
24) 박찬영, 김현식 (2024), 앞의 글, pp. 178-179.
25) 작년 해킹 80%는 '북한발'…"방산의 'ㅂ'만 들어가면 다 턴다", 디지털데일리 (2025.04.18), 〈https://www.ddaily.co.kr/page/view/2025041816382130656〉
26) 정부지원 해킹조직 '금성121', '북한 선교학교 신청서'로 위장해 APT 공격중, 데일리시큐, (2019.06.17.), 〈https://www.dailysecu.com/news/articleView.html?idxno=53038〉
27) "보안 취약한 교회·종교단체 해킹 표적 되기 쉽다", 국민일보 (2023.12.31.), 〈https://www.kmib.co.kr/article/view.asp?arcid=0019021039〉

표적으로 삼고 있음을 미루어 짐작할 수 있다.

이러한 북한의 노골적인 위협은 우리에게 다시 한번 사역 현장에서 보안의 중요성을 일깨워준다. 과거 선교 현장의 정보 보안의 주요 이슈는 부주의와 실수로 인한 우발적인 정보 유출의 위험이 주된 것이었고, 주로 체류하는 선교사가 주의해야 할 이슈로 여겨지곤 했다. 그러나 이제는 악성코드가 담긴 이메일 유포, 스마트폰을 대상으로 한 해킹 문자나 메신저를 통한 정보 유출 시도, 각종 SNS를 통한 사회공학적 해킹 등 직접적으로 교회나 사역 후원자를 대상으로 한 공격 사례가 발생하고 있다. 이러한 공격은 대체로 의식하지 않는다면 쉽게 속아 넘어갈 수밖에 없는 내용으로 위장되어 있기 때문에 평소 이런 위협에 대한 경계가 없다면 큰 피해를 당할 수 있다. 확대되는 북한의 사이버 공격과 날이 갈수록 교묘해지는 공격 기법에 대한 우리의 주의가 요구된다. 이러한 사회공학적 해킹 외에도 기술적 취약점을 활용한 직접적인 해킹 피해도 증가하고 있다. 기술적 공격은 일선 교회 수준에서 대비하기엔 제한적이지만, 빠른 보안 업데이트와 2차 비밀번호 이용 등을 통해 그 위협을 최소화하는 노력이 필요하다.

다소 맥락에서 벗어난 이야기일 수 있지만, 북한의 사이버 공격이 교회와 성도들에게까지 영향을 미치는 불편한 현실이 오히려 북한 선교에 무관심했던 교회와 성도들에게 북한을 향한 관심과 기도를 일깨우는 계기가 되기를 바란다. 북한이 교회를 겨냥해 사이버 공격을 감행하는 배경에는 오랫동안 이어져 온 뿌리 깊은 기독교에 대한 적대감과 극심한 박해가 자리하고 있다. 북한은 체제 유지와 통제를 위해 기독교를 위협적인 존재로 간주하고, 신앙을 가진 사람들을 가혹하게 탄압해 왔다. 이러한 현실은 북한 내부에서 기독교가 결코 사라지지 않았으며, 오히려 당국이 두려워할 만큼 영향력을 지니고 있음을 보여준다. 북한의 교회를 향한 공격도 그만큼 복음의 파급력을 우려하고 경계하기 때문일 것이다. 따라서 우리는 북한의 사이버 범죄를 비판하거나 교회의 보안 의식을 강화하는 데에만 머물러서는 안 된다. 남한의 교회는 때때로 북한 문제나 통일 문제, 그리고 북한에서 비밀리에 신앙을 지키고 있는 형제자매들의 삶에 대해 무관심할 수 있다. 그렇지만 이제는 북한이 드러내는 기독교와 교회에 대한 적대감을 직시하고, 이를 통해 고통 속에서도 신앙을 지키고 있는 형제자매들을 위해 기도와 연대의 자리로 나아가야 한다. 북한의 공격은 우리에게 위협이자 도전이지만, 동시에 신앙 공동체가 북한을 향한 관심과 사랑을 회복하는 계기가 될 수 있다. 이제는 우리가 북한의 상황을 깊이 인식하며 기도와 행동으로 응답해야 할 때이다.

칼럼 1

총 대신 키보드를 든 군대 : 북한 사이버전의 실체와 우리의 대응

이 상 용 (데일리엔케이 AND센터 디렉터)

요즘 한국 사회 곳곳에서 이상한 사건이 잇따르고 있다. 예배 도중 화면에 인공기가 나타나거나, 인권단체가 보낸 메일이 해킹당하고, 심지어 암호화폐 거래소가 털리는 일도 벌어졌다. 이런 사건의 뒤에는 하나의 공통점이 있다. 바로 북한 '해커 조직'이다.

오랫동안 이 문제를 추적해 온 전문가들은 북한의 사이버 공격은 단순한 기술 범죄가 아니라고 말한다. 그들은 총 대신 키보드를 들고, 전쟁 대신 인터넷 공간에서 싸운다는 것이다.[1)]

이와 관련 최근 다국적 제재 모니터링팀인 MSMT는 보고서를 통해 북한 해커들이 2024년 한 해 동안 약 28억 달러(한화 약 3조 8000억 원)에 달하는 암호화폐를 훔쳤다고 밝혔다.[2)] 이 돈은 핵 개발과 군사 자금, 그리고 사이버전 운영비로 쓰이고 있다고 할 수 있다. 즉, 사이버 공간은 이제 북한 정권의 새로운 전쟁터가 된 셈이다.

'정찰정보총국' : 김정은 시대의 정보전 사령부

북한은 당군정 여러 조직이 이 같은 사이버 공간을 악용해 여러 활동을 하고 있지만 일단 최근 확대 개편된 '정찰정보총국'을 주목할 필요가 있다. 데일리NK

1) 정보보안회사 레코디드 퓨처의 지정학적 위협정보 분석가인 스콧 카르다스는 지난 8월 한 토론회에서 이를 두고 '회색지대 전쟁'(gray zone warfare)이라고 평가한 바 있다.

2) The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities, https://msmt.info/Publications/detail/MSMT%20Report/4221

내부 소식통에 따르면, 이 조직은 위성(IMINT), 신호(SIGINT), 사이버, 인적정보(HUMINT)를 한데 묶은 '정보전 사령부' 역할을 담당한다고 한다.[3] 김정은 국무위원장이 직접 주도한 이 개편(지난 6월 말 최종 확정)은 "전쟁은 총으로만 하는 게 아니라, 정보와 데이터로도 한다"는 구상을 실현한 것이다.

이에 따라 정찰정보총국은 단순히 해커 부대를 관리하는 곳이 아니게 됐다. 위성 감시, 전자전, 사이버 해킹, 외화벌이를 하나의 체계로 묶은 종합 정보기관이라는 뜻이다. 그 안에서 해커들은 군사정보를 수집하고, 동시에 돈을 벌어들이는 "경제형 정보전사"로 움직인다. 즉, 북한의 해킹은 군사행동이자 외화벌이 수단이라는 뜻이다.

표 1. 정찰총국 정보전 운용 구조

분 야	주요 임무	비고
IMINT(위성)	기상·지형·기지 변동 감시, 변화탐지 중심	만리경-1호 운용
SIGINT(신호정보)	교신·레이더·훈련패턴 수집, 위성 큐잉(queuing) 제공	위성 수집보완 역할
HUMINT(인적정보)	항만·군수시설 등 폐쇄공간 내 정황 수집	'그림자 정보' 확보
CYBER/OSINT	정보수집·해킹·외화조달· 제재회피	정보본부 핵심 축으로 편입

정찰정보총국의 이런 변화는 단순히 조직 개편이 아니라, 북한이 '정보'를 무기로 삼는 시대에 들어섰다는 신호다. 예전에는 총이나 미사일이 국가의 힘을 보여주는 수단이었다면, 이제는 데이터와 정보, 그리고 이를 조작하고 훔칠 수 있는 능력이 곧 권력이라고 할 수 있다. 김정은 정권은 해커를 단순한 기술자가 아닌, 경제와 군사를 동시에 책임지는 전사(戰士)로 키우고 있는 셈이다. 해킹으로 얻은 정보는 외화벌이에도 쓰이고, 정치·군사 전략 수립에도 활용된다. 다시 말해, '정보전'이 '경제전'과 '심리전'을 아우르는 형태로 진화하고 있는 것이다.

여기서 또 하나 간과하지 말아야 할 부분은 이 조직의 핵심이 바로 해외로 파견된 북한 IT 노동자들이라는 점이다. 그들은 합법 비자나 유학, 기술 연수 명목으로 중국·러시아·동남아 등 30여 개국에 흩어져 있는 것으로 전해진다. 겉보기에는 단순한 프로그래머이지만, 실제로는 정찰정보총국의 지시에 따라 일하고 있는 셈이다. 이들은 온라인 플랫폼을 통해 전 세계 기업의 프로그램 개발에 참여하고, 그 과정에서 얻은 돈을 북한 당국에 상납하고 있다. 또한 일부는 기업의 내부 시스템에 침투해 정보를 빼내거나, 해킹을 위한 통로를 미리 만들어 둔다.

이와 관련 MSMT 보고서도 "북한 IT 인력이 가짜 신분으로 해외 기업 프로젝트에 참여하고 있다"라고 경고하고 있다. 이런 활동을 통해 벌어들인 외화는 다시 북한으로 흘러 들어가, 해킹 장비와 제재 회피 자금으로 쓰이는 것이다.

표 2. 해외 IT 노동자 및 사이버전력 연계

분 야	내 용
파견형태	합법 비자·유학·기술연수 위장파견
활동지역	중국·러시아·동남아·남미 등 30여국
수익모델	프리랜서 플랫폼을 통한 원격 개발
보고체계	외화 수익은 총국 자금망으로 환류, 정보 수집 병행
활용목적	외화 조달, 산업정보 접근, 사이버 침투 기반 확보

사이버 전쟁의 그림자, 보이지 않는 감시와 통제

북한의 사이버 공격은 세 가지 목표로 나뉜다. 첫째, 돈을 벌기 위한 공격이다. 암호화폐 거래소, 은행, 개인 투자자를 노려 외화를 확보한다. 둘째, 정보를 빼내기 위한 공격이다. 한국의 정부 기관, 언론사, 종교 단체, 인권 단체가 주요 표적이라고 할 수 있다. 북한은 이들을 통해 한국 사회의 움직임과 대북 정보 활동을 파악하고 있다. 셋째, 심리전이다. 가짜뉴스를 퍼뜨리고, 사회 갈등을 부추기며, 북한 비판 단체의 신뢰를 떨어뜨리는 셈이다. 최근에는 인공지능을 활용해 가짜 영상을 만들거나, 실제 인물처럼 위장한 해킹 메일을 보내는 사례도 늘고 있다. 이처럼 북한의 사이버전은 단순한 범죄가 아니라 체제 생존을 위한 전면전에 가깝다는 점도 중요한 대목이다.

문제는 북한의 사이버전 뒤에는 인권 유린의 현실이 숨겨져 있다는 점이다. 해외로 파견된 IT 노동자들은 스스로 일하는 자유로운 개발자가 아니다. 그들은 가족이 북한에 남아 있고, 상납을 거부하면 가족이 처벌당하는 구조 속에 있다. 하루 12~16시간씩 일하고, 벌어들인 돈 대부분을 국가에 바친다. 숙소는 늘 감시 아래 있고, 인터넷 사용과 통신은 제한된다고 한다. 보위부 요원이 함께 생활하며 이메일과 메신저까지 통제한다. 실질적으로 이들은 현대판 '사이버 노예'와 다름없다. MSMT 보고서도 "북한의 해외 IT 인력은 단순한 외화벌이 수단이 아니라, 체계적 인권 침해의 한 형태"라고 지적하고 있다. 결국 북한의 해커 한 명 한 명 뒤에는, 자유를 빼앗긴 노동자의 그림자가 드리워져 있는 것이다.

다시 말해 그들은 당국이 내린 비밀 임무를 수행하는 사람들로, 하루하루 감시와 통제 속에서 살아가고 있다. 감시요원이 항상 곁을 지키며, 개인적인 판단이나 의견을 말하는 것은 꿈도 꿀 수 없는 것이다. 특히 직접 사이버 공간을 누비는 조건이다 보니 이메일 내용이나 여러 접속 기록도 철저히 감시당하고, 숙소나 이동

3) 이상용, 데일리엔케이, "정찰정보총국, 위성·사이버 정보까지 통합한 '정보전 지휘탑'", 2025년 10월 17일, https://www.dailynk.com/20251017-6/

경로까지 정해져 있다고 한다.

만약 이들이 탈출을 시도하면 그 대가는 매우 가혹한다고 한다. 현장에서 총살될 수 있다는 공포(실제로 김 위원장은 이 같은 지시를 하달한 바 있다고 한다)[4], 그리고 북한에 있는 가족이 함께 처벌받는다는 두려움이 늘 따라다닌다. 일종의 연좌제다. 아울러 파견 기간 중 문제가 생기면 다시는 해외로 나갈 수 없고, 가족도 정치적 불이익을 받을 수도 있다. 그래서 이들은 언제나 두려움 속에서 일을 계속해야 하는 것이다.

파견 전후로, 지속적으로 '사상 교육'이라는 이름의 세뇌 과정도 그들을 괴롭히는 요소 중 하나다. IT 노동자들은 김일성·김정일주의를 반복적으로 외우고, "적국의 문화에 물들지 말라"는 경고를 계속 듣고 있다. 이처럼 공포와 세뇌가 결합된 환경에서, 북한의 IT 노동자들은 자유를 잃은 채 명령만 수행하는 기계처럼 일하고 있다. 결국 그들의 노동은 정권의 외화벌이 수단으로 이용되고 있는 셈이다.

방심이 부르는 침투…인식 확산이 곧 방어선

그렇다면 우리는 제대로 된 대처를 보여주고 있다고 할 수 있는가? 안타깝지만 한국은 여전히 북한의 사이버 공격에 제대로 대응하지 못하고 있다는 게 중론이다. 공공기관은 그나마 시스템이 있지만, 교회, 언론사, 인권 단체는 보안 사각지대다. 심지어 공공기관도 뚫리는 경우가 많다.

특히 북한이 제재의 틈을 뚫고 꾸준히 기술 발전을 꾀하고 있다는 점도 주목된다. 일단 최근 북한은 러시아와의 기술협력을 통해 위성 추진체, 센서, 지상국 운영 등 핵심 분야의 기술 발전을 꾀하고 있다. 정찰정보총국 내부에는 러시아 전문가와 접촉하는 전담 부서가 생겼고, 군사기술 자문 형태의 협력이 이미 진행 중인 것으로 알려졌다. 러시아의 위성·전자전 경험이 북한의 정찰·공격 능력 강화로 이어질 가능성이 크다.

이와 동시에 북한은 라오스, 베트남, 남미 등 제3국 지역에서도 정보망과 자금 조달 네트워크를 넓히고 있다. 이는 단순한 외화벌이를 넘어, 국제 금융망과 기술 인프라 속으로 자신들의 정보 조직을 녹여 넣으려는 시도로 풀이된다. 제재를 피해 새로운 통로를 만들고, 외화와 기술을 동시에 확보하려는 복합 전략이라 할 수 있다.

특히 중국과의 협력은 한층 공고해지고 있다. 중국의 지방정부나 민간기업을 통해 상용 전자부품과 데이터 처리 기술을 제공받으면서, 이를 '민수(民需) 거래'로 위장해 감시망을 피하고 있다. 심지어 최근 북한 당국이 '조중(북중)기술합작센터'를 설립하고 중국 주요 도시에 IT 인력 선발대를 파견한 정황도 포착되고 있다.[5] 중국과 러시아뿐 아니라 동남아시아까지 이어지는 이런 협력망은 북한이 제재를 돌파하며 기술 수준을 빠르게 끌어올리는 배경이 되고 있다. 결과적으로 북한은 사이버전과 정찰 기술을 결합한 '기술형 위협 국가'로 변모하고 있으며, 이는 국제사회의 새로운 골칫거리로 부상하고 있다.

이런 점에서 우리 정부는 미·일 등 국제사회와 함께 정보 공유를 강화하고, 북한 IT 인력의 해외 활동을 추적해야 한다. 또한 사이버 보안뿐 아니라 인권 차원의 대응도 함께 이뤄져야 한다. 북한의 해킹은 단순한 기술 문제가 아니라, 노동 착취와 체제 유지를 위한 범죄이기 때문이다.

우리의 일상으로 돌아와 보면 피싱 메일 한 통, 낯선 링크 클릭 하나가 북한 해커의 통로가 될 수 있다. "보안의 허점은 기술이 아니라 사람의 방심에서 시작된다"라는 말을 가슴 깊숙이 새겨야 한다. 북한의 사이버전은 이미 우리 일상에 파고들었다. 총소리는 들리지 않지만, 피해는 현실이다. 그들의 공격은 기술로 막을 수도 있지만, 더 중요한 것은 인식의 변화다. 각 기관과 시민이 보안의 중요성을 알고 경계심을 갖는 것, 그것이 곧 우리의 방어선이라고 할 수 있다.

부록 1. 해킹 예방 10대[6] 수칙

1. 운영체제·프로그램을 항상 최신 버전으로 업데이트하세요.→ 보안패치가 해킹 차단의 첫 걸음입니다.
2. 백신(안티바이러스) 프로그램을 설치하고 실시간 감시 기능을 켜두세요.
3. 중요 자료는 정기적으로 외부 저장장치나 클라우드에 백업하세요.
4. 비밀번호는 8자 이상·영문+숫자+특수문자 조합으로 만들고, 2단계 인증(2FA)을 설정하세요.
5. 출처가 불분명한 이메일이나 문자 링크·첨부파일은 열지 마세요.
6. 공식 홈페이지를 직접 입력해 접속하고, 이메일 링크를 통한 로그인은 피하세요.
7. 공용 와이파이 사용 시 금융·업무 정보 입력은 절대 하지 마세요.
8. 관리자 계정은 별도로 사용하고, 불필요한 서비스나 포트는 차단하세요.
9. 피싱·메신저 사칭 등 금전 요구는 반드시 전화로 재확인하세요.
10. 해킹·랜섬웨어 의심 시 즉시 인터넷 연결을 끊고 '118(보호나라)'로 신고하세요.

4) 기획취재팀, 데일리엔케이, "[그물에 갇힌 인권] "北, IT 노동자 탈북 시 현장 처형 규정" ", 2025년 2월 19일, https://www.dailynk.com/20250219-6/

5) 정태주, 데일리엔케이, "김정은 방중 후 '북중기술합작센터' 설립…기술협력 탈 쓴 외화벌이", 2025년 10월 24일, https://www.dailynk.com/20251024-5/

6) 한국인터넷진흥원(KISA)은 정기 업데이트와 2단계 인증을 가장 기본 수칙으로 권고한다.

칼럼 2

북한 ICT 발전과 그 위험성

곽 인 옥 교수 (통일경제사회연구소 소장)

1. 기술과 통제의 역설

세계에서 가장 폐쇄적인 국가 중 하나인 북한이 소프트웨어 분야에서 강력한 역량을 보유하게 된 현상은 하나의 지정학적 역설을 제기한다. 하드웨어 산업 기반이 취약하고 인터넷 접근이 극도로 제한된 체제임에도 불구하고, 북한은 국제 수준의 프로그래머와 사이버 전문가를 체계적으로 양성해 왔다. 이 현상은 단순한 기술 발전을 넘어, 독재 체제의 생존 전략과 깊이 연관되어 있다.

본 글에서는 북한의 소프트웨어 강국화 전략을 단순한 산업 정책이 아닌, 체제 안보, 국제 제재 회피, 지식 엘리트 통제, 그리고 생존 경제의 디지털화가 정교하게 결합된 '하이브리드 생존전략'이라는 핵심 분석틀을 통해 조명하고자 한다. 북한의 IT 역량은 고립된 기술 섬이 아니라, 국가의 생존과 직결된 핵심 자산으로 기능하며, 이 보고서는 그 구조와 작동 방식, 그리고 지정학적 함의를 분석하는 것을 목표로 한다.

따라서 이 글은 북한의 IT 전략을 국가 안보, 경제적 생존, 그리고 지정학적 함의라는 세 가지 차원에서 심층적으로 분석할 것이다. 이를 통해 폐쇄 사회가 기술을 어떻게 생존과 통제의 도구로 활용하는지에 대한 통찰을 제공하고자 한다. 다음 장에서는 이러한 전략이 어떻게 국가 차원에서 설계되고 제도화되었는지 그 기원을 살펴볼 것이다.

2. 국가 주도 IT 전략의 기원과 구조

북한의 IT 전략은 단순한 산업 정책이 아니라 국가의 최상위 안보 및 생존과 직결된 '국가 전략'으로 설계되었다. 이는 북한의 디지털 역량을 이해하는 데 있어 가장 중요한 출발점이다. 경제적 효율성이나 시장 논리가 아닌, 체제 보위와 국가 생존이라는 절대적 목표 아래 모든 자원과 인력이 동원되는 구조이기 때문이다.

이러한 전략의 사상적 기반은 1990년대 중후반으로 거슬러 올라간다. 당시 김정일은 "21세기의 경쟁력은 프로그래밍과 수학에 있다"라고 언급하며 '지식경제화' 노선을 천명했다. 이 선언 이후 북한은 "지식은 무기이며, 프로그래머는 병사"라는 인식하에, IT 및 소프트웨어 전략을 국가 안보의 하위 개념으로 편입시켜 발전시켰다.

이 전략을 뒷받침하는 핵심 기관들은 인재 양성부터 기술 개발, 군사적 활용에 이르기까지 유기적으로 연결되어 있다.

이처럼 북한의 IT 정책은 처음부터 철저히 국가 안보와 체제 유지를 위한 도구로 설계되었다. 이러한 구조를 유지하는 핵심 동력은 바로 다음 장에서 다룰 독특한 인재 양성 시스템에서 나온다.

3. '디지털 전사' 양성 시스템: 영재교육의 군사화

북한의 IT 강국화는 고도로 체계화된 조기 영재 발굴 및 교육 시스템에서 비롯된다. 이 시스템은 단순한 교육 정책을 넘어, 체제에 절대적으로 충성하는 기술 엘리트를 길러내는 '국가형 인재 사육 시스템'이자, 인재 자체를 국가의 자원으로 관리하는 '인재 관리 기술(technologies of human cultivation)'로서 기능한다.

● 조기 선발과 집중 교육

북한은 초등학교 단계부터 수학, 물리, 프로그래밍에 재능을 보이는 학생들을 조기에 선발하여 특별 관리한다. 금성제1중학교, 평양제1중학교, 김책공업대학 부속중학교 등은 국가가 지정한 대표적인 'IT 영재학교'이다. 이들 학교에서는 일반 과목의 비중을 줄이는 대신, 수학, 알고리즘, 암호학, 그리고 C, Python, Java와 같은 프로그래밍 언어를 집중적으로 교육한다.

이러한 교육의 강도와 목적은 한 탈북 IT 전문가의 증언을 통해 생생하게

드러난다.

> *"우리는 14살 때부터 12시간씩 컴퓨터 앞에 앉았다. 학교는 감옥 같았지만, 성적이 좋으면 평양에 남을 수 있고, 나중에 외화벌이팀이나 해커 조직에 갈 수 있었다."*
> *— 탈북 IT 전문가 (2022년 인터뷰, 서울)*

이 증언은 북한의 영재교육이 개인의 성취를 위한 기회인 동시에, 국가가 제시하는 특권을 얻기 위한 치열한 경쟁의 장임을 보여준다. 즉, 영재교육은 '엘리트의 특권'과 '체제 충성의 시험장'이라는 이중적 성격을 지닌다. 이러한 극한의 압박과 보상 구조는 단순히 기술적 역량만을 평가하는 것이 아니라, 국가의 목표에 헌신할 수 있는 이념적 순응성까지 시험하여 고도로 숙련되고 사상적으로 통제된 '디지털 전사'를 단련시키는 과정이다.

● 군사화된 교육 경로

영재학교를 졸업한 인재들은 대부분 국방대학, 자동화연구소, 조선콤퓨터센터(KCC) 등으로 진학하며, 최종적으로는 민간기업이 아닌 군 및 정부 산하 조직에 배속된다. 이들이 배치되는 곳은 사이버전을 담당하는 '121국'이나 '조선엑스포'와 같은 대외 기술 무역 및 해킹조직이다.

2020년 미국 재무부 제재보고서에 따르면, 약 6,000명에 달하는 북한 IT 전문가가 군·정부 산하 조직에 소속되어 있으며, 이들 중 상당수가 제3국에서 원격으로 외화벌이를 수행하고 있는 것으로 나타났다. 이는 북한의 영재교육 시스템이 단순한 인재 양성을 넘어, 국가의 전략적 목표를 수행하는 '디지털 전사'를 양성하는 군사화된 시스템임을 명확히 보여준다.

4. 경제 생존 전략으로서의 IT: '보이지 않는 수출국'의 작동 방식

이처럼 국가에 의해 길러진 인재들이 어떻게 국제 제재를 우회하며 경제적 생존 수단을 확보할까? 국제사회의 강력한 제재 속에서 북한은 소프트웨어 개발 및 사이버 활동을 통해 독자적인 외화벌이 구조를 구축했다. 이는 자원의 물리적 한계를 '지식 노동의 익명성'으로 대체하여, 북한을 사실상의 '보이지 않는 노동 수출국'으로 변모시킨 핵심 생존 전략이다.

특히 2015년 이후, 북한 개발자들은 중국, 러시아, 인도 등 제3국에서 신분을 위장한 '프리랜서'로 활동하며 제재망을 효과적으로 회피해왔다. 이들의 활동 방식은 합법과 불법의 경계를 넘나들며 다양한 형태로 나타난다.

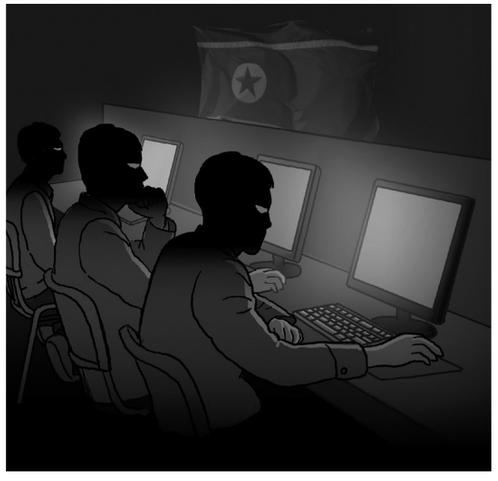
▶사례 1: 합법 시장 침투 (미국 법무부, 2018) 북한 개발자들이 중국인 명의를 도용한 유령회사를 설립해 애플 앱스토어에 iOS 게임을 출시하고 수익을 송금한 사례는 이들의 정교한 전략을 드러낸다. 이는 단순히 기술력을 과시하는 것을 넘어, 국제 금융 시스템과 기업법, 신분 위장 기술을 포함한 고도의 작전 보안(OPSEC) 능력을 바탕으로 합법적인 글로벌 플랫폼에 침투하여 제재를 무력화하는 능력을 입증한다.

▶사례 2: 대규모 불법 해킹 (블룸버그, 2021) 라자루스 그룹이 암호화폐 거래소를 공격해 약 4억 달러를 탈취한 사건은 사이버 범죄가 국가 재정의 핵심 수단으로 활용되고 있음을 보여준다. 이는 단순한 해킹이 아니라, 정권 유지와 대량살상무기 개발 자금을 직접 조달하기 위한 '국가 주도형 대규모 약탈(state-sponsored grand larceny)'이다. 북한은 전 세계 금융 시스템 자체를 정권의 생존을 위한 자원 추출 대상으로 삼고 있는 것이다.

▶사례 3: 글로벌 하청 경제 편입 (탈북 IT인, 2023) 평양 개발자들이 실리콘밸리 소스코드를 참고하며 외주 업무를 수행했다는 증언은 이들이 기술적으로 고립되어 있지 않음을 시사한다. 오히려 이들은 높은 기술 경쟁력을 바탕으로 글로벌 소프트웨어 공급망의 최하단에 익명으로 편입되어 있다. 이는 합법적인 프리랜서와 북한의 '디지털 노동'을 구별하기 어렵게 만들어, 제재 이행에 심각한 도전 과제를 제기한다.

5. 사이버 전력화와 비대칭 위협: '코드로 무장한 군대'

이러한 경제 활동은 단순한 외화벌이를 넘어 필연적으로 군사적 목적과 결합 된다. 북한의 소프트웨어 역량은 경제적 생존 수단을 넘어, 국가 차원의 비대칭 군사력으로 전환되었다. 재래식 군사력의 열세를 극복하기 위한 저비용·고효율의 전략적 카드로 사이버 역량을 적극 활용하고 있다. 북한의 사이



버 공격은 경제적 이득과 전략적 보복이라는 이중 목적을 갖는 '국가 차원의 비대칭 무력 수단'으로 규정할 수 있다.

북한의 사이버 전력은 목적과 기능에 따라 분화된 핵심 조직들을 통해 운용된다.

조직들의 활동은 단순한 범죄 행위를 초월하는 전략적 의미를 갖는다. 라자루스 그룹의 금융 해킹은 외화벌이를 넘어 국제 금융 시스템을 교란하는 압박 수단으로 기능하며, 블루노로프와 안다리엘의 산업 기밀 탈취는 군사기술 격차를 줄이고 국가 기간산업을 위협하는 비대칭 공격이다. 이처럼 북한은 사이버 공간을 제재에 대한 보복과 국제사회에 대한 전략적 압박을 가하는 전장으로 활용하고 있다. 이는 북한이 소프트웨어 기술을 통해 실질적인 '코드로 무장한 군대'를 운용하고 있음을 명백히 보여준다.

6. 종합 분석 : '평양 하이브리드 생존경제'와 디지털 통제

지금까지 분석한 국가 전략, 인재 양성, 경제 활동, 군사화를 어떻게 통합적으로 이해할 수 있을까? 북한의 IT 전략을 구성하는 각 요소들을 통합적으로 분석하기 위해서는 독특한 이론적 틀이 필요하다. 북한의 영재교육 시스템은 단순히 인재를 키우는 것을 넘어 국가의 생존을 위한 '인지자본(cognitive capital)'을 생산하는 체계로 작동한다. 이 구조 안에서 개별 인재는 독립된 주체가 아니라, 국가가 필요에 따라 투입하고 관리하는 '알고리즘적 자원'으로 취급된다.

이러한 독특한 시스템을 본 저자는 '평양 하이브리드 생존경제(PHSE: Pyongyang Hybrid Survival Economy)' 이론을 통해 설명하고 있다. 이 이론에 따르면, 북한의 생존 경제는 시장경제적 요소와 국가통제적 요소가 기이하게 결합된 하이브리드 시스템이다. 북한의 소프트웨어 부문은 이 이론의 가장 대표적인 사례로, 다음 세 가지 요소가 복합적으로 작동한다.

▶시장적 합리성: 외화벌이와 기술 수출이라는 명확한 목표 아래, 시장의 수요에 맞는 기술과 인력을 공급하며 경제적 이익을 추구한다.

▶국가적 통제: 양성된 모든 인력과 그들이 생산하는 정보, 기술을 국가가 철저히 독점하고 통제하여 이익이 체제 외부로 유출되는 것을 막는다.

▶군사적 활용성: 경제 활동을 통해 축적된 기술과 인력은 언제든지 사이버 전력으로 전환되어, 국가의 비대칭 안보 역량을 강화하는 데 활용된다.

이처럼 북한의 IT 전략은 시장, 국가, 군사 논리가 하나의 시스템 안에서 모순 없이 작동하는 독특한 생존 모델이다.

7. 21세기형 '디지털 독재'의 함의

이 복합적인 하이브리드 시스템이 궁극적으로 지향하는 바는 무엇인가?, 그리고 이것이 북한 체제와 국제사회에 어떤 의미를 갖는가? 북한의 소프트웨어 강국화 전략은 단순히 기술적 성취를 의미하지 않는다. 이는 기술 발전, 엘리트 충성 유도, 외화 확보, 그리고 체제 안보라는 네 가지 목표가 정교하게 맞물려 작동하는 복합적인 생존 메커니즘이다. 이 시스템을 통해 북한은 과학기술의 발전을 체제 유지와 권력 재생산의 핵심 도구로 활용하는 '디지털화된 통치 방식'을 구축했다.

결론적으로, 북한의 IT는 "시장경제의 언어로 말하는 전체주의의 코드"라고 규정할 수 있다. 겉으로는 글로벌 시장의 기술과 방법론을 따르지만, 그 본질은 체제 생존과 통제라는 전체주의적 목표에 철저히 복무하기 때문이다.

이처럼 세계에서 가장 폐쇄된 사회가 지식과 기술을 무기로 국제무대에서 생존을 도모하는 이 현상은, 북한을 21세기형 "디지털 독재의 실험장"으로 이해하는 중요한 창을 제공한다. 이는 기술 발전이 반드시 사회의 개방이나 민주주의로 이어지지 않을 수 있다는 중요한 지정학적 함의를 우리에게 던져주고 있다.

칼럼3

북한 사이버 범죄의 진화

양 운 철 (세종연구소)

2025년 6월 18일 서울 온누리교회(서빙고 캠퍼스)와 내수동교회의 새벽 예배 유투브 생중계 도중 북한의 인공기가 화면에 나타나는 사건이 발생했다. 북한의 사이버 범죄는 세계적으로 문제가 된 지 오래지만, 한국 교회를 대상으로 한 북한의 사이버 해킹은 매우 충격적이다. 특히, 탈북자를 돕는 해외 선교사들에 대한 감시와 위협은 계속 증가하고 있다. 오랫동안 북한은 한국의 종교 단체, 종교 지도자, 대북 인권 단체 등에 대해 다양한 방식으로 해킹을 시도해 정보를 수집하고 있다. 한국의 국내 정치에도 관여해 정치적 분열과 혼란을 일으키고 있다. 문제는 빠르게 발전하고 있는 북한의 사이버 기술이 이런 악한 일에 사용되고 있다는 점이다. 이에 대한 한국 교회의 대처가 필요하다. 하나님의 간섭만이 북한을 변화시킬 수 있다는 문제의식을 바탕으로 북한의 사이버 범죄 발전 과정을 분석해 본다.

북한 사이버 해킹의 급속한 확산

북한은 계획경제의 모순으로 늘 물자 및 외화 부족에 시달리고 있다. 2025년 현재도 북한 원화의 미국 달러화 대비 환율은 계속 증가하고 있다. 외화가 필요한 북한으로서는 외환 보유를 늘리기 위해서는 높은 수익을 제공하는 불법 사이버 범죄 행위를 선택할 수밖에 없었다. 북한은 해외 금융기관 해킹, 암호화폐(crypto-currency) 탈취, 랜섬웨어(ransomware)를 통한 금품 갈취 등 다양한 방법으로 외화를 불법적으로 획득하고 있다.

북한의 사이버 공격 능력은 핵과 같은 위협적인 비대칭 전략으로 간주한다. 사이버 위협의 효과는 상대적으로 크기 때문에 북한은 사이버 부문의 역량을 강화하는 전략을 계속 추진하고 있다. 핵 보유는 국제적 감시가 심하고 높은 비용을 수반하지만, 사이버 전력의 강화는 상대적으로 효과 대비 비용이 적기 때문이다.

북한이 한국에 대한 사이버 공격을 시작한 정확한 시점을 지정하기는 어렵다. 그러나 북한이 2009년 시도한 한국 국가 기관에 대한 네트워크 해킹 사건이 큰 충격을 준 점은 분명하다. 이후 2011년 국가 기관 망을 공격한 디도스(DDoS) 공격, 2014년 한국수자원공사 해킹, 2016년 국방망과 방산 기업 해킹, 2017년 비트코인 거래소 해킹 시도, ATM기기 해킹, 2021년 한국항공우주산업과 한국원자력연구원에 대한 해킹 사건이 연속적으로 발생했다. 이런 일련의 사건은 북한으로서는 저비용으로 최대의 효과를 얻을 수 있는 공세였다. 북한으로서는 사이버 범죄가 한국을 견제할 수 있는 최고의 수단이었다. 사이버 범죄는 북한 내부 선전용으로도 사용되고 있다. 북한 주민들에게 체제의 과학적, 군사적 우월성의 이미지를 강화하고, 기술적으로도 강대국에 맞설 수 있는 능력을 지니고 있다고 선전하고 있다.

북한의 사이버 범죄는 해외에서도 활발히 진행되고 있다. 북한은 2014년 미국에 있는 SONY 영화사(SONY Pictures Entertainment Inc)를 해킹했다. 이때만 하더라도 국제사회는 북한의 사이버 해킹 기술이 예상보다는 뛰어나지만, 큰 위협 대상으로는 간주하지 않았다. 그러나 2016년 2월, 북한이 뉴욕 연방은행의 방글라데시 중앙은행 계좌에서 미화 8,100만 달러를 탈취한 사건은 전 세계를 놀라게 했다. 당시 북한은 아시아의 설 연휴와 미국의 주말 시간대를 노려 범행을 진행했다. 해킹당한 현금 중 1,450만 달러는 필리핀에서 회수했지만, 나머지 6천6백만 달러는 회수에 실패했다. 탈취한 돈은 필리핀의 여러 카지노로 송금된 후, 다단계로 세탁이 되어 찾기가 어렵게 되었다. 이 사건으로 자신을 얻은 북한은 더욱 적극적으로 금융 해킹을 수행하게 되었다. 북한은 이후에도 워너크라이(WannaCry) 랜섬웨어 사건을 주도했고, 다양한 가상화폐 거래소를 해킹하여 암호화폐를 탈취하기도 했다.

북한의 무차별적인 해킹은 한국에서도 많은 문제를 일으켰다. 2017년 3월, 북한의 해커 조직이 국내의 ATM 63대에서 약 24만 건의 전자금융 거래 정보를 탈취했다. 국내 불법 조직은 거래 정보를 중국교포로부터 전달받아 한국, 미국,

일본, 중국, 태국, 대만 등 6개국 범죄 조직에 전달했고, 526장의 복제 카드를 만들어 불법적으로 사용했다. 유사한 사례로, 북한의 해커들이 국내 범죄 조직과 결탁하여 사이버 범죄에 개입한 사례도 있다. 2011년 국내 범죄 조직이 북한 해커들과 공모하여 리니지와 같은 인기 높은 온라인게임 서버를 해킹해 게임 아이템을 수집하는 프로그램을 제작, 배포하여 거액을 탈취하기도 했다. 미국 재무부는 2024년 5월에 공개한 "대체불가토큰(NFT) 관련 불법 금융 리스크 평가 보고서"에서 북한이 2022년 1년 동안 가상자산 절취로 한화로 약 1조 원에 달하는 가상자원을 탈취했다고 공표했다. 인지도가 높은 기관이나 조직으로 위장한 전자 우편을 보내 개인의 정보를 탈취하기도 한다. 이 경우, 가장 단순한 수단으로 해킹을 당하기도 한다. 대표적 사례가 백도어를 통한 해킹이다.

암호화폐 탈취에 집중

해외 자산 탈취를 위해 북한은 비용대비 수익이 가장 큰 사이버 금융 범죄를 목표로 정했다. 타 국가의 자산을 불법적으로 탈취하는 사이버 범죄 활동은 국가가 큰 노력을 들여 양성한 해킹 그룹에 의해 수행된다. 북한은 여러 제약에도 불구하고 사이버 금융 범죄에 전력을 기울이고 있다. 관련하여 국제사회의 북한에 대한 경제제재 강화와 불법행위에 대비하는 수단도 발전되었다. 블록체인 연구 회사인 Chainalysis에 따르면, 암호화폐 관련 산업의 회사들에서 도난당한 총금액이 2021년에 33억 달러에서 2022년 약 38억 달러로 증가했다고 발표했다. Chainalysis는 대부분의 해킹 활동이 북한군과 관련된 집단에 의해 주도되었다고 지적한 바 있다.

북한의 사이버 불법행위가 증가할수록, 국제사회의 방어 기제도 진화하게 된다. 현재 북한이 집중적으로 탈취하려는 가상자산(virtual asset)은 컴퓨터나 인터넷에서 저장되는 데이터 또는 디지털 금융자산을 의미한다. 가상자산은 암호화폐로 표현되기도 하며, 또는 블록체인, 분산원장기술, 암호화에 기반을 둔 디지털 금융자산을 총칭하기도 한다.[1] 가상화폐가 제 기능을 가지려면 블록체인, 암호화, 분산원장기술이 필요하다.

분산원장(distributed ledger)은 복제, 공유 또는 동기화된 디지털 데이터에 대한 합의 기술이다. 이때 관련 데이터는 여러 사이트나, 국가 또는 기관 등에 분산된다. 즉, 중앙집중적인 관리자나 데이터 저장소가 없어도 데이터 기능은 작동하게 된다. 만약 사용자들이 직접 접속(peer-to-peer)하는 네트워크가 있다면, 관리 비용은 급속히 감소하게 된다. 원리는 음원이나 영화 사이트에서 공유하고 있는 자료를 서로 내려받는 원리와 거의 유사하다. 이러한 설계의 대표적인 사례는 블록체인 시스템이다. 현실에서 일반인들은 은행에 대한 신뢰가 있어, 은행제도와 같은 중앙집중 원장(centralized ledger)을 이용해 왔다. 개인이 은행에 수수료(신뢰 비용)를 지급하면, 은행은 고객들의 금융 자료를 보관하고, 금융서비스도 제공한다. 반면 은행 서비스는 비용을 요구하며, 절차상 일정 시간이 소요된다. 각 은행은 상호 간의 데이터베이스를 통해 거래를 확인하고 청산한다. 이 과정에서 자료는 중앙은행이나 금융결제원 등을 경유하기도 한다. 외환 송금이나 무역 대금 결제는 더욱 많은 기관과 관계자가 관여하게 된다.

그러나 개인이 분산원장기술(Distributed Ledger Technology)을 사용하게 되면, 집중화된 중앙원장 해킹 사례와 달리, 개인은 중앙서버나 중앙관리자의 제어 없이 분산화된 네트워크에서 개인이 사용하는 데이터베이스를 공유하고 동기화도 할 수 있다. 그 이유는 특정인을 해킹하더라도 그 개인에 대한 정보가 많은 사람에게 암호화되어 분산, 저장되었기 때문이다. 블록체인은 중앙서버가 아닌 분산된 네트워크에서 관리되기 때문에 네트워크의 모든 참여자는 같은 원장을 가지고 있다. 따라서, 모든 참가자는 신뢰할 수 있는 은행이 없어도 데이터를 안전하게 관리할 수 있게 된다.

북한의 가상자산 해킹에 대한 제제

2022년 북한과 연계된 해커들이 탈취한 가상자산 액수는 약 17억 달러로 역대 기록을 경신했다. 2023년에 디 파이(DeFi) 플랫폼으로부터 탈취한 가상자산은 약 4억 2천8백만 달러이고, 중앙화 서비스(targeted centralized services)로부터 1억 500만 달러, 거래소로부터 3억 3,090만 달러, 지갑공급업체(wallet providers)로부터 1억 2,700만 달러를 탈취했다.[2] 반면 미국의 해외자산통제국(OFAC)은 2022년 8월 라자루스 그룹의 자금 세탁을 도운 토네이도 캐시(Tornado Cash)를 제재 대상으로 지정했다. 2023년 11월 미국의 해외자산통제국은 북한의 라자루스 그룹이 가상자산에서 탈취한 자금을 세탁한 비트코인 믹서 신밧드를 폐쇄했다. 당시 신밧드의 가상자산 입금액은 8억

1) 삼정KPMG 경제연구원, Business Focus: 가상자산, 금융 생태계의 새로운 패러다임, 2022년 8월. p. 5.

2) Chainalysis, The Chainalysis 2024 Crypto Crime Report. p. 43.

2,140만 달러에 달했다.

이 사례를 보면, 북한의 금융자산 해킹은 상당히 성공했지만 실제로 훔친 가상자산을 현금화하는 작업은 전혀 다른 문제이다. 북한이 사이버 공격, 불법 무역, 암호화폐 해킹 등을 통해 자금을 확보하더라도, 이를 합법적인 금융 시스템으로 전환하는 데에는 많은 제약이 있다. 미국과 UN의 강력한 제재로 인해 북한과 연관된 자금의 이동은 철저하게 감시를 받고 있다. 특히, 방글라데시 중앙은행 해킹 사건 이후, SWIFT와 같은 국제 금융 네트워크는 북한과의 거래를 차단하고 있다. 공식적으로 북한의 금융기관이나 관계자들이 국제 금융 시스템에 접근하는 것은 매우 어렵다. 그리고 여러 국가가 북한의 불법 자금 세탁을 막기 위해 금융기관에 대한 자금세탁방지(AML: Anti Money Laundering) 규정을 강화하고 있다. 금융기관들의 의심스러운 거래에 대한 감시로 인해 북한의 정상적인 금융 시스템을 통한 현금화는 거의 불가능하게 되었다.

북한의 큰 수입원이었던 암호화폐 거래소 해킹은 여러 국가의 규제 강화로 인해, 탈취한 암호화폐를 법정화폐로 전환하는 과정이 매우 어려워졌다. 그동안 북한을 간접적으로 지원했던 중국과 러시아도 북한을 지원할 경우 국제사회의 압력을 받기 때문에 공식적인 도움을 주기는 어려운 현실이다. 암시장을 통한 현금화도 국제거래 대부분이 추적 가능해지면서, 잘 실현되지 못하고 있다.

국제사회도 북한의 자금 세탁과 현금화 시도를 막기 위해 정보 공유 및 협력 체제를 강화하고 있다. FATF(자금세탁방지 금융대책기구)는 북한을 고위험 국가로 지정하고, 북한과 연관된 금융 거래를 금지하거나 엄격히 규제하도록 권고하고 있다. 따라서 북한의 자금 이동은 실시간으로 추적되고, 금융기관이 의심 거래를 발견하면 즉시 차단할 수도 있다. 국제 제재와 감시 강화로 인해 북한과 거래를 해오던 대리인들도 위험 부담이 높은 북한과의 거래를 지속하기는 어렵다. 만약 북한이 불법 자금을 현금화하려면 매우 큰 거래비용을 부담해야만 한다.

북한이 탈취한 암호화폐를 중국 브로커를 통해 현금화한다는 내용의 보도도 있었다.[3] 그러나 액수가 클수록 현금화는 어려우며 부대 비용도 큰 폭으로 증가하여 정상적인 거래로 유지되기는 어려울 것이다. 최근 북한은 불법 자금의 현금화를 위해 믹싱(mixing) 서비스를 사용하고 있다. 믹싱은 글자 뜻처럼 여러 사람이 입금한 가상화폐를 한곳에 섞은 뒤 발급된 인증 코드로 어디서든 찾아갈 수 있는 서비스이다. 비록 북한이 입금자와 출금자의 연결고리를 끊어 추적을 어렵게 하더라도, 특정 국가의 정부가 자국의 가상화폐 거래소를 조사, 감시하면, 현금화는 거의 불가능하게 된다. 북한으로서는 아직은 익명성이 보장되는 암호화폐를 탈취하여, 비밀리에 현금화하려 할 것이다. 그러나 이에 대한 국제사회의 대응도 계속 발전하기 때문에, 북한이 다른 국가나 국민의 자산을 훔쳐, 현금화하는 작업은 계속 어려워질 것으로 예상한다. 동시에 이에 맞서는 북한의 대응 전략도 발전해 나갈 것이다. 이에 대한 국제사회의 감시와 대비가 절실한 시점이다.

맺는 말

북한의 사이버 범죄 기술과 전략은 상당히 빠르게 진화하고 있다. 2000년대 초기에는 한국에 대한 정찰, 감시, 교란을 집중적으로 수행했다. 2013년 이후에는 금융 해킹에 집중한 것으로 추정된다. 외국 은행 해킹, SWIFT 네트워크 해킹, 멜웨어 공격이 확대되었다. 2017년부터는 암호화폐를 포함한 가상자산 탈취에 집중하였다.

이런 사실은 수십 년 동안 경제적 어려움에서 벗어나지 못하고 있는 북한의 계획경제와 너무 대조된다. 북한은 사이버 범죄 분야에 상당한 경쟁력을 갖추고 있으며, 관련 종사자들에게도 어느 정도의 인센티브가 제공되고 있다고 추정된다. 그렇지만 북한의 사이버 범죄에 대한 국제사회의 감시가 강화될수록 북한의 수익 창출도 감소하게 될 것이다.

3) RFA, "전 FBI 관리 "북, 중국 브로커 통해 탈취 암호화폐 현금화," 2024.8.29.

특별칼럼

AI시대, 교회와 선교단체의 보안에 대하여

심 영 근 선교사 (기술과학전문인선교회 FMnC 대표)

AI로 인해 엄청난 변화를 겪고 있는 시대, 우리는 눈에 보이지 않는 전쟁을 경험하고 있습니다. 과거의 전쟁이 총과 칼의 충돌이었다면, 오늘의 전쟁은 데이터와 계정, 네트워크를 노리는 보이지 않는 공격으로 이루어집니다. 해커들은 AI를 이용해 우리의 음성을 흉내 내고, 공동체의 문체를 베껴 정교한 피싱 메일을 만들며, 선교지의 정보와 교회의 계정을 노립니다. 이는 단순한 기술 문제가 아니라, 하나님께서 맡기신 공동체와 선교적 대의을 지키기 위한 영적 청지기로서 가져야 할 사명의 문제가 아닐지 생각합니다. 현대를 살아가는 우리에게 새롭게 요구되는 자세는 깨어 있는 보안 의식일 것입니다.

2025년 6월, 서울의 한 유명 대형 교회에서 새벽예배가 유튜브로 생중계되던 중 갑자기 화면이 바뀌었습니다. 설교자의 음성이 끊기고, 대신 북한 인공기가 화면에 등장했고, 북한 국가로 추정되는 곡이 흘러나왔습니다. 온라인으로 예배하던 성도들은 충격을 받았고, 교회는 단순 장비 오류가 아니라 외부 해킹 가능성을 진지하게 조사 중이라고 밝혔습니다.

사건 자체는 몇 분의 해프닝처럼 지나갔을지 모릅니다. 그러나 그 몇 분은 우리에게 이러한 질문을 던집니다. "우리가 보안의 문제를 외면하게 된다면 일상의 예배조차 지켜낼 수 없는 시대가 된 것은 아닐까?"

2023년, 대한예수교장로회 통합 소속 서울의 한 대형 교회는 코로나 시기 랜섬웨어 공격을 받았습니다. 교인들의 이름, 생년월일, 주소, 전화번호, 직분 등 방대한 개인정보가 암호화되었고, 해커는 돈을 요구했습니다. 교회는 성도들의 삶을 아주 잘 알고 있는 공동체입니다. 주일학교의 아이들 정보부터 성도들의 이름과 연락처, 직장 정보까지 자연스럽게 모입니다. 이 모든 것이, 해커의 눈에는 "돈이 되는 데이터"입니다. "개인정보 많은 교회… 불구경할 때 아니다"라는 어느 신문 기사의 제목처럼, 한국 교회가 더 이상 '나는 작은 교회라서 괜찮다'라고 말할 수 없는 시대가 되었습니다.

위협은 단지 개인정보 유출이나 예배 방해에 그치지 않습니다. 2019년, 북한과 연계된 해킹 조직 '김수키(Kimsuky)'가 인천의 한 교회 서버를 해킹해, 그 서버를 숙주 삼아 정부의 안보·외교 라인을 향한 공격을 시도한 정황이 적발된 바 있습니다. 교회의 서버는 해커에게 좋은 "우회 통로"입니다. 종교 기관이라는 특성상 보안 투자가 상대적으로 적고, 신뢰가 높은 도메인이라 각종 기관과의 메일과 문서 교환이 많기 때문입니다. 어떤 해커에게는 교회의 서버가 곧 "국가 시스템을 향한 비밀 통로"인 셈입니다.

선교 현장도 예외가 아닙니다. 북한 배후 해킹조직이 안드로이드 스마트폰과 PC를 원격 조종해 사진, 문서, 연락처 등 데이터를 통째로 삭제하거나 탈취한 사례가 최근 국내 보안 분석 보고서에서 확인되기도 했습니다. 스마트폰 하나에 선교사의 연락망, 동역자 리스트, 사역 사진, 현지 성도들의 정보까지 들어 있는 시대에, 이런 공격은 단순한 '기술 사고'가 아니라 '사역 전체의 붕괴 위험'이 될 수도 있음을 우리는 경각심을 가지고 인지해야 할 것입니다.

요즘 한국 언론에는 "교회·목사 사칭 주의보"라는 제목의 기사들이 빈번히 등장합니다. 2025년 1월 제주에서 적발된 한 사기 조직은 목회자를 사칭해 중고 거래 사이트에서 고가의 이동식 농막·컨테이너를 판매하는 것처럼 속여 돈을 가로챘습니다. 이들은 목사라는 신분이 주는 신뢰를 악용해 피해자들을 안심시켰고, 대포통장으로 돈을 받은 뒤 사라졌습니다. 또 다른 사례에서, 사기범은 부목사를 사칭해 교회의 대규모 공사를 맡길 것처럼 접근했습니다. 그리고 설비업체에 "교회를 위해 자동심장충격기(AED) 50대를 선결제 해주면, 나중에 공사 대금과 함께 현금으로 정산해 주겠다"고 유도했습니다. 심지어 교회 홈페이지에 아직 등록되지 않은 '부임한 지 며칠 안 된 부교역자의 이름'을 도용하고, 가짜 명함까지 만들어 사용하는 치밀함을 보였습니다. 이제 해킹과 사기는 '교회 바깥세상 이야기'가 아니라, 예배당 안, 목양실 안, 단체 카톡

방 안으로 들어와 있습니다. 그리고 AI는 이런 사기를 한층 더 정교하게 만들 수 있는 도구가 되었습니다.

최근 국내 보안 전문 매체 '포티넷'의 조사에 의하면, 한국 내 조직 10곳 중 7곳(70%)이 지난 1년간 AI 기반 사이버 위협을 경험했으며 특히 응답자의 62%는 위협이 2배로 증가했다고 답했고, 30%는 무려 3배로 늘어났다고 응답했다고 합니다. 이 통계 속에 "교회와 선교단체"라는 이름은 따로 적혀 있지 않았지만, 보안에 취약하면서도 개인·재정·네트워크 정보가 많이 모여 있는 조직이라는 특징을 생각해 보면, 이 수치는 교회와 선교 단체에게도 그대로 적용될 가능성이 큽니다. AI는 이제 해킹 도구를 만드는 데에도 사용됩니다. 공격자는 AI에게 교회 홈페이지, 주보, SNS 글을 읽히고, 그 공동체의 말투와 신앙적 표현까지 학습시킨 뒤, 더욱 정교한 피싱 메일과 메시지를 만들어냅니다. "샬롬"으로 인사도 하고, "헌신과 순종"이라는 단어를 어색하지 않게 쓰는 "해커"가 등장한 셈입니다.

마태복음 10장에서 예수님은 제자들에게 이렇게 말씀하십니다.

"뱀 같이 지혜롭고 비둘기 같이 순결하라."

순결과 지혜가 동시에 요청됩니다. 이 말씀을 따라 우리는 정보 보호 차원에서 교회 내에서 어떻게 적용해야 할까요? 우리는 악을 두려워하지 말되, 악의 방식에 대해 무지해서도 안 될 것입니다. 오늘날 보안은 단지 IT 부서의 업무가 아니라, 청지기의 책임입니다. 하나님이 우리에게 맡기신 사람, 정보, 사역, 네트워크를 정직하고 지혜롭게 관리하는 일입니다. 보안은 불신만이 동기가 된 것이 아닙니다. 보안은 사랑의 또 다른 이름이라고 부를 수 있을 것입니다. 사랑하기 때문에 쉽게 노출되지 않도록 하고, 소중하기 때문에 공격으로부터 무방비로 두지 않는 것입니다.

그렇다면, 무엇부터 바꾸어야 할까요? 감성적인 경고만으로는 실제 사고를 막을 수 없습니다. 여기서 우리는 전문가들과 공공기관, 글로벌 보안 조직들이 한목소리로 반복해 온 조언을 귀 기울여 들어야 합니다. 가장 먼저 적용할 것으로 거의 모든 전문가가 한결같이 말하는 것은 "다중 인증(MFA)"입니다. '다중 인증(Multi-Factor Authentication, MFA)'은 비밀번호 외에 추가적인 확인 단계를 요구해 보안을 강화하는 로그인 방식입니다. 클라우드 서비스와 보안 관련 자료를 제공하는 AWS는 다중 인증(MFA)을 "비밀번호가 도난당하더라도 무단 접속을 막아 주는 추가 보안 계층"이라고 설명합니다. 한국 인터넷진흥원(KISA)이 운영하는 보안 정보 사이트 역시 2단계 인증 전용 앱을 사용하면 짧은 시간마다 번호가 바뀌기 때문에, 해킹 위험에서 벗어날 수 있다고 안내합니다. 국내 인터넷 인프라 기업 가비아는 해외 사이버보안 교육기관 SANS의 보고서를 인용하며, "다중 인증(MFA)을 통해 사이버 보안 사고의 99.9%를 예방할 수 있다"라고 소개합니다. 마이크로소프트는 자사 보안 문서에서 "연구 결과, MFA는 계정 탈취 공격의 99.2% 이상을 차단할 수 있다"라고 밝힙니다. 또 다른 문서에서는 "탈취된 계정의 99.9% 이상이 MFA를 사용하지 않고 있었다"라고 덧붙입니다. 미국 사이버보안·인프라보안국(CISA)은 공식 자료에서 "MFA는 당신을 훨씬 더 안전하게 만들어 준다"라고 강조하며, 단순 비밀번호만 사용하는 관행을 "나쁜 보안 습관"으로 분명히 지적합니다. 요약하면, 세계 곳곳의 보안 전문가들과 기관들은 모두 같은 말을 합니다. "우선, MFA부터 적용시켜야 한다." 교회와 선교단체도 예외가 될 수 없습니다. '대표 이메일', '회계 담당 계정', '선교지와 주고받는 메신저 계정', '예배·영상 송출 계정' 등은 반드시 MFA를 적용해야 합니다. 비밀번호 하나에 사역 전체가 달려 있는 구조는, 더 이상 신뢰의 문제가 아니라 위험한 관리입니다.

한국인터넷진흥원(KISA)이 운영하는 정보보호 관리체계(ISMS)는, 조직이 관리적·기술적·물리적 보호 조치를 통합적으로 갖추어야 한다고 설명합니다. 자동차 산업에서는 이와 유사한 개념으로 '사이버보안 관리체계(CSMS)'가 등장해, 앞으로는 자동차 제작사도 필수적으로 이런 보안 체계를 갖추어야 할 것으로 전망합니다. 이는 우리에게 중요한 힌트를 줍니다. "보안은 특정 기술 하나를 도입하는 것으로 끝나는 것이 아니라, 관리 체계로 이어져야 한다"라는 것입니다.

교회와 선교단체가 취할 수 있는 최소한의 관리체계를 5가지로 정리해 보았습니다. 2025년을 기준으로 제시된 관리 체계를 실행하면 95% 이상 보호가 가능하다고 봅니다.

1. 모든 계정에 2단계 인증(MFA) 100% 적용

오늘 당장 해야 할 일 1순위입니다. 구글·네이버 등의 이메일, 홈페이지 관리자, 헌금 프로그램, 카카오톡까지 예외 없이 2단계 인증을 적용해야 합니다. 최근 3년간 한국 교회 유튜브 해킹의 99%가 MFA 미적용 때문에 발생했다고 합니다. 설정은 10분이면 충분하고, 비용은 전혀 들지 않습니다. 하지만 보안 효과는 절

대적입니다.

2. 중요 데이터는 주 1회 자동 백업 & 오프라인 보관

교인 명부, 헌금 내역, 설교 영상, 선교지 정보 등은 외장하드나 NAS에 암호화 백업 후 교회나 단체의 외부에도 한 부 보관하세요. 랜섬웨어가 와도 몸값 없이 복구 가능합니다. 한 번 설정하면 자동으로 진행되므로 초기 설정만 신경 쓰면 됩니다.

3. 비밀번호 강력하게 & 피싱 교육 분기 1회

비밀번호는 12자리 이상으로 정하며 90일마다 변경하는 것이 좋습니다. 비밀번호 관리 도구를 사용하여 관리할 것을 권장합니다. 전 직원·봉사자에게 "유튜브 수익 정산", "헌금 확인" 같은 가짜 피싱 메일 실전 훈련을 실시합니다. 한국 교회 해킹의 70% 이상이 약한 비밀번호 또는 피싱 클릭 때문이라고 합니다. 기술보다 사람을 먼저 준비시켜야 합니다.

4. 홈페이지·공유기 기본 보안 & KISA 무료 점검 활용

홈페이지의 워드프레스 플러그인은 최신 버전으로 유지합니다. 공유기 관리자의 계정(admin)과 비밀번호를 주기적으로 변경합니다. 공용 와이파이와 사무실 네트워크는 분리합니다. 매년 KISA 118 전화로 '내서버돌보미' 무료 진단 받을 것을 추천합니다.

5. 사고 발생 시 즉시 대응 프로세스 미리 준비

예방도 중요하지만, 사고 발생 시 신속한 대응은 피해를 최소화합니다. 해킹·랜섬웨어 의심 시에는 ① 감염 PC의 전원을 끄고 네트워크선을 뽑습니다(추가 확산 차단). ② KISA 118 또는 112에 신고합니다(전문가 지원 요청). ③ 백업으로 복구를 시작합니다(사전에 준비한 백업 활용). 위급 상황에서는 누구에게 전화해야 할지 몰라 시간을 낭비하는 경우가 많습니다. 명확한 연락 순서를 눈에 보이는 곳에 붙여두면, 누구든 즉시 대응할 수 있습니다.

작은 실천이 교회나 단체의 소중한 데이터와 성도들의 개인정보를 지킵니다. 지금 바로 시작하는 것이 중요합니다. 또한 퇴사자·사역 종료자의 권한은 즉시 회수하는 것도 잊지 않는 것이 좋습니다. 선한 관계로 떠났더라도, 계정과 권한은 정리해야 합니다. 이는 불신이 아니라, 남은 사람을 보호하는 기본 수칙입니다.

AI가 새로운 공격 도구로 사용되고 있는 만큼, 교회와 선교단체 안에서도 AI를 둘러싼 몇 가지 공동체 규칙이 필요합니다. 첫째, AI에게 무엇을 절대 말하지 않을 것인가를 정해야 합니다. 선교지 위치, 구체적인 인명·연락처, 후원자 리스트, 민감한 재정 정보 등은 어떤 생성형 AI에도 입력하지 않겠다는 내부 원칙이 필요합니다. 둘째, 음성·영상 지시는 반드시 다른 채널로 재확인합니다. 대표자의 음성이 담긴 전화로 “지금 급하게 송금해달라”는 요청이 오면, 문자나 별도의 공식 채널로 다시 확인하는 절차를 의무화해야 합니다. 딥페이크는 더 이상 공상과학이 아닙니다. 셋째, AI가 작성한 이메일과 문서를 ‘무조건 신뢰’하지 않아야 합니다. AI는 설득력 있게 거짓을 구성할 수도 있습니다. 내용뿐 아니라 수신자와 링크를 두 번 확인하는 습관이 필요합니다. 넷째, AI 활용 자체를 막기보다는 ‘경계선’을 분명히 정해야합니다. 설교 정리, 홍보 문구 초안, 일반 행정 문서의 초안 등은 활용하되, 민감한 정보와 연결되는 작업은 반드시 사람의 판단 아래 제한해야 합니다. 이러한 규칙은 우리가 AI를 두려워해서가 아니라, AI를 도구로 사용하되, 영적 분별력을 잃지 않기 위해 필요한 “경계선”입니다.

북한 연계 해킹조직이 교회 서버를 거점 삼아 정부망을 공격하려 했고, 대형 교회의 새벽예배 영상이 해킹으로 조작되었으며, 선교단체와 교회의 계정들이 단지 ‘보안이 약하다’는 이유만으로 표적이 되는 시대입니다. 우리는 하나님이 맡기신 공동체를 사랑하기 때문에 정보를 함부로 다루지 말아야 합니다. 목회자 혼자, IT 담당자 혼자, 회계 담당자 혼자서 보안에 대해 노력하는 것만으로는 우리의 소중한 정보와 사람들의 안전을 지킬 수 없습니다. 목회자는 강단에서 “보안도 영적 청지기직의 일부”임을 선포할 수 있습니다. 선교사는 자신의 기기와 계정을 보호하는 구체적 훈련을 받을 수 있습니다. 행정 담당자는 관리 체계를 정리하고 문서화할 수 있습니다. IT 담당자는 MFA, 백업, 암호화, 로그 모니터링 등 기술적 조치를 설계할 수 있습니다. 이사회와 당회, 운영위원회는 보안 예산과 정책을 사치가 아니라 필수로 받아들일 수 있습니다. 이렇게 모두가 협력하고 자신의 역할들을 돌아본다면 앞으로 더 큰 분별력이 필요해지는 공격 앞에서 지켜야 할 것을 최선으로 지켜낼 수 있을 것입니다.

AI시대의 보안은, 기술의 가장자리에 있는 부가 옵션이 아니라, 하나님이 맡기신 사명을 다음 세대까지 안전하게 전달하기 위한 필수적인 청지기직입니다. 우리가 함께 지혜를 모으고 힘을 모아 “디지털 보안”이라는 “안전한 울타리”를 세울 때, 하나님께서 이 시대의 교회와 선교단체에 맡기신 복음의 사명이 훼손되지 않고, 새어 나가지 않고, 막히지 않고, 더 멀리, 더 깊이 땅끝까지 흘러가게 될 것입니다.

탈북민 인터뷰

복음이 이 땅의 소망입니다

– 인천한나라은혜교회 김권능 목사 (하) –

편집부

올해는 광복 80주년을 맞는 해입니다. 광복의 그 날을 주신 주님께 감사를 올려드리면서 동시에 그 기쁨을 제대로 누리기도 전에 분단의 아픔을 경험했던 우리의 가슴 아픈 역사를 생각합니다. 그러한 역사의 굴곡 가운데서 한반도 기독교 신앙의 중심이었던 북한 교회가 현재까지 겪고 있는 고초와 고난, 그리고 그럼에도 그 땅의 영혼들을 잊지 않으시고 역사하고 계신 하나님의 손길도 아울러 되새겨 봅니다.

북한개발소식에서는 탈북민 목회자로서 인천한나라은혜교회를 담임하고 계신 김권능 목사님을 만나 그분의 신앙 여정과 북한을 향한 비전을 듣는 시간을 가졌습니다. 인간의 헤아림을 초월하시는 북한의 영혼들을 향한 하나님의 손길을 느낄 수 있는 시간이었습니다. 목사님의 나눔이 독자님의 마음에 북한에 대한 복음의 소망과 하나님의 일하심에 대한 신뢰가 자라나는 기회가 되길 바라며 지면을 통해 해당 내용을 3회에 걸쳐 나눕니다.

5) 한국행과 목회자의 길

감옥 생활을 마치고 북송이 예정되어 있었는데, 기적적으로 피하셨다고 들었습니다.

사실 북송이 되었어야 했는데 하나님께서 신비하게 역사해 주셨습니다. 석방이 될 시기에 김정일이 사망하면서 북한의 국경이 막힌 것입니다. 그로 인해 북송이 이루어지지 않으면서 한국으로 올 수 있게 되었습니다. 시한부 인생이었는데 생명을 덤으로 더 받은 셈입니다.

한국에 들어오셨을 때부터 교회 사역의 비전을 가지고 계셨나요? 어떻게 남한에서 목회자의 길을 걸어가시게 되었나요?

한국에 막 도착할 즈음에는 쉬고 싶다는 생각이 간절했습니다. 그동안 가족을 살려야 한다는 부담감에 시달렸고, 그리스도인이 된 후에는 부족하지만 나라와 민족, 주님을 위해 살고자 애썼고, 감옥에서 수년간 감시받는 삶을 살았으니 이제는 조용하게 살면서 몇 년은 쉬어야겠다고 생각했습니다. 중국에서는 일을 해도 신분 때문에 월급도 제대로 받지 못하고 자주 쫓기며 살았는데 대한민국에서는 그럴 걱정이 없으니 일하면서 제대로 월급도 받으면서 평범하게 살아보고 싶다는 생각도 있었습니다.

그런데 하나원을 퇴소하자마자 중국에서 저를 가르치셨던 최광 선교사님께서 저를 데리고 신학교에 당장 들어가야 한다고 하셨어요. 원래 입학 수속은 일정이 중요하잖아요. 만약 1년 쯤 기다려야 한다는 타이밍이었다면 일정을 핑계로 취업을 했을 겁니다. 그런데 마침 9월에 퇴소를 해서 그 달 말까지 입학 수속 해야만 했어요. 그래서 엉겁결에 퇴소 하자마자 급하게 입학 수속을 진행했고, 감사하게도 총신대에 진학하게 되었습니다.

취업을 하는 것이 나쁜 일은 아니지만 몇 년을 그렇게 생활하다 보면 사명을 따라 목회의 길로 가기는 힘들었을 것 같습니다. 그래서인지 하나님께서는 제가 다른 길로 가지 않도록 인도하셨어요. 입학 원서는 제출한 후에도 재정의 문제가 있었습니다. 이제 막 입국을 한 터라 등록금이 없었거든요. 그래서 다시 1~2년 정도 일을 해서 등록금을 벌어야겠다고 생각하고 양천구 남부고용청에 가서 이력서를 냈고, 며칠 후에 채용 연락을 받았어요. 그런데 마침 채용 연락을 받기 전날에 선교사님께 연락을 받았어요. 저의 학비를 지원해주시겠다는 후원이 들어왔다는 거에요. 신학교를 가게 되더라도 등록금 벌기 위해서 1~2년 정도는 일을 할 생각이었는데 정말 절묘한 타이밍에 연락이 교차하더군요. 하나님의 인도하심을 인정하지 않을 수 없었어요. 그리고 감옥생활을 통해 하나님의 뜻은 피할 수 없음을 체감했기 때문에 인도하심에 순종했습니다. 주변에서는 일하지 않고 공부를 시작한 저를 무책임하게 보는 시선도 있었지만, 하나님의 뜻은 순종해야 한다는 생각으로 신학을 공부하고 목회를 시작했는데, 그런 결정을 할 수 있었던 것은 10년의 감옥 생활 덕분인 것 같습니다.

6) 한국 교회와 북한 지하교회

밖에서 보시던 한국 교회와 직접 사역자가 되시고 경험하신 한국 교회는 아무래도 차이가 있으셨을 것 같습니다. 한국 교회를 직접 경험하시면서 느낀 점이 있으시다면 무엇일까요?

처음 대학원에 진학하고 한국 교회를 경험할 때에는 마음이 힘들었습니다. 북한에 대해 다들 무관심하다고 느껴졌기 때문입니다. 감옥에서 저를 지탱해 준 말씀 중에 시편 102편 17~22절이 있습니다. "이는 갇힌 자의 탄식을 들으시며 죽이기로 정한 자를 해방하사 여호와의 이름을 시온에서, 그 영예를 예루살렘에서 선포하게 하려 하심이라"(20~21절). 갇힌 자의 탄식을 들으시는 여호와께서 북한도 굽어보시고 살펴보시고, 그 탄식을 들으시고 해방하실 것을 믿음으로 말씀을 암송했었습니다. 그런데 남한에 와서 보니까 남한 교회가 하나님의 관점에서 북한을 바라보고 긍휼한 마음을 품기보다는 북한을 불편하고 멀리 두고 싶은 존재로 느끼는 것 같았습니다. 남한 교회 안에 이념 갈등이나 전쟁의 트라우마가 아직까지 영향을 미치고 있는 것 같았고, 그래서인지 해외의 기독교인들은 북한과 북한선교에 대해 더 순수하게 받아들이는데 비해 우리는 아직 넘지 못한 벽이 있는 것 같은 느낌을 받았습니다.

이런 점에서 단순히 북한의 문이 빨리 열리는 것이 능사가 아니라는 생각도 들었습니다. 우리 안에 이러한 상처와 무관심을 극복하지 못한다면 문이 열려도 과거의 증오심에 갇히게 됩니다. 그래서 저는 남한 교회도 하나님의 긍휼하심이 필요하고 그 안에서 상처가 치유되고 회복되어야 하지 않을까 생각해 봅니다.

그래도 감사한 점은 한국 교회가 오랜 기간 헌신된 모습도 보였다는 것입니다. 고난의 행군 당시 남한도 IMF로 힘들었지만 교회가 선교사 파송하고 지원한 덕분에 저희가 복음을 들었지 않았습니

까? 현재 북기총 소속 50여개 탈북민 교회가 있는데, 이렇게 탈북민 목회자가 일어나고 교회가 일어난 것에는 한국 교회의 노력이 있었음에 감사하고 있습니다. 아무리 부족해도 교회가 세상 양심보다는 훨씬 낫다고 생각합니다. 교회가 희망입니다. 그래서 저희 교회 주보에는 "한국교회는 대한민국과 열방의 희망입니다." "한국교회는 고난당하는 북한주민들의 희망입니다." "나는 한국교회의 희망입니다." 라고 우리의 고백을 실었습니다. 북한을 향한 트라우마와 세상 풍조에 갇히지 않길 바라는, 우리를 향한 구호입니다.

앞서 복음을 통해 변화되셨던 목사님의 삶을 들었기 때문인지 교회가 희망이라는 말씀이 더욱 마음에 와닿는 것 같습니다. 교회에 대해 이야기하다 보니 남한의 교회뿐 아니라 북한의 지하교회에 대해서도 생각하게 됩니다. 특히 목사님께서는 중국에 계실 때 탈북자 복음 사역에 참여하셨던 만큼 복음을 듣고 돌아간 이들에 대한 마음이 남다르실 것 같습니다. 목사님께서는 북한의 지하교회를 어떻게 바라보고 계신가요?

종종 한국 교회 내에서도 북한 지하교회의 존재를 인정하지 않는 분들이 보입니다. 물론 북한 지하교회에 대해 어떤 수치나 규모에 집착하는 모습은 바른 접근은 아니라고 생각합니다. 그렇지만 하나님께서 바알에게 무릎 꿇지 않은 칠천 명을 북한에 남겨두셨다는 사실을 믿습니다. 저는 중국에서 그리스도를 영접하고 다시 고향으로 돌아가 가족들에게 복음을 전한 사람들을 여럿 알고 있습니다. 북한 사람들이 많이 탈북했던 90년대 말에서 2000년대 초반에는 중국에도 부흥이 있었습니다. 각 촌마다 교회가 세워지고 예수 믿는 사람들이 늘어났습니다. 그리고 이 교회들이 탈북자에게 먼저 도움의 손길을 내밀었기 때문에 탈북자들 대부분이 복음을 접했고, 한 번도 못 들었다고 하는 사람은 극소수에 불과합니다. 그중에 많은 이들이 다시 고향으로 돌아가서 살고 있습니다. 척박한 북한의 환경에서는 하나님을 모르는 사람도 하늘을 찾게 되곤 합니다. 그렇다면 복음을 들은 사람은 당연히 주님을 찾지 않겠습니까? 저는 해방 전에 예수를 믿었던 그루터기 신앙의 뿌리 1세대들이 90년대 즈음에는 대부분 돌아가셨을텐데, 하나님께서 이 시기에 새로운 복음의 불씨를 당겨주신 것은 아닐까 생각하곤 합니다.

어떤 이들은 복음을 듣고 돌아간 탈북자들 대부분이 단지 도움을 받기 위해 믿는 척을 했을 뿐이라고 이야기합니다. 그런 사람들도 당연히 있겠지만 진정으로 거듭난 신앙인이 되어 돌아간 경우도 많습니다. 제 친구는 북한에서 헌병이었는데 여기와는 다르게 북한은 헌병이 일반 주민을 수색할 수 있습니다. 그 친구 말로는 90년대 주민 수색에서 성경책이 여럿 발견되었었다고 합니다. 누군가가 말하는 것처럼 교회의 도움 받은 탈북자들이 강변에 자신들이 받은 성경이나 신앙 자료를 버리기도 했지만, 또 다른 누군가는 위험을 무릅쓰고 북한까지 가지고 들어갔던 것이지요. 또 한 번은 특정 지역 보위부가 자기 지역에 숨어 있는 지하 성도를 잡으려고 거꾸로 중국 교회 쪽으로 사람을 보내 역추적을 시도한 사실을 발견한 사례도 있습니다. 보위부에서 사람을 보내서 "중국의 어느 교회에 가서 거기 사역자와 접촉하면서 우리 지역에 연결하는 사람을 알아봐라, 그 교회가 지하교회 사역을 하고 있다."라고 지령한 것이지요. 북한이 이런 활동을 벌인다는 것은 역으로 북한에 지하교회가 실존한다는 사실을 보여줍니다.

지하교회 교인의 수준과 자질을 문제 삼는 이들도 있습니다. 북한 지하교회는 어쩔 수 없는 많은 제약이 있습니다. 마음껏 예배드릴 수 없고, 우리가 누리는 신앙 교육이나 훈련, 교사들, 성경이나 신앙 자료도 턱없이 부족합니다. 그렇지만 그들은 가장 열악한 상황 속에서도 주님의 이름을 부르고 있고, 하나님밖에 의지할 것이 없는 가운데 하나님께서 허락하시는 초대교회의 역사를 체험하기도 합니다. 어떤 면에서는 기성 교회에서 볼 때 너무 체험적이라거나 이단적인 요소가 없는지 주의해야 할 부분도 있겠지만, 그들이 신자인지 아닌지를 따지는 일이 먼저가 되어서는 안 된다고 생각합니다. 극심한 박해 상황에서도 주님을 찾는 그들을 품고, 존중하고, 함께 가야지요. 판단하는 마음보다는 열린 마음, 긍휼한 마음, 도우려는 마음이 있어야 한다고 생각합니다.

7) 비전과 소망

목사님의 말씀을 들으며 북한을 향한 열정과 함께 하나님의 일하심에 대한 신뢰가 느껴집니다. 현재 목사님께서는 인천한나라은혜교회를 담임하시면서 귀한 사역을 감당하고 계시는데요, 앞으로의 사역의 비전을 나눠주실 수 있을까요?

사람을 모으고 목표를 달성하는 그런 것이 보통 비전으로 이야기되곤 하지만, 저의 신앙 여정에서 하나님께서는 그런 수치적인 목표와는 상관없는 삶을 살게 하셨습니다. 하나님의 뜻이 온전히 이루어지기를 기도하고, 우리의 몫은 순종이라고 생각합니다. 하나님 앞에 내어드림이 우리의 목적이라고 믿습니다.

처음 교회 개척을 고민할 때 하나님께서는 선교의 열매는 결국 교회라는 사실을 깨닫게 하셨습니다. 북한을 바라볼 때에도 강퍅한 사람들을 억압에서 벗어나게 하고 굶주린 이들에게 밥을 먹이는 것도 중요한 목적이지만, 생명의 말씀으로 교회가 회복되는 것이 하나님의 계획이라고 믿습니다. 이런 측면에서 남한식 자유는 우리의 방법일 수도 있겠다는 경계도 해봅니다. 우리가 북한을 향해 나아갈 때 가지고 가야 할 것은 자본주의 사회의 그것이 아니라, 자본주의 사회에서도 많은 유혹과 난관을 이겨내고 하나님을 간증하는 우리 탈북민 성도의 삶, 그리고 부모의 신앙의 모범을 배우고 성장하는 우리의 자녀들의 모습이라고 생각합니다. 우리의 삶을 바꾸지 못한 복음은 그들에게도 복음이 아닐 것입니다. 그래서 하나님을 따르는 성도의 모습을 고스란히 북한으로 가져가는 것이 전도라고 생각합니다. 이것은 한 개인으로는 할 수 없습니다. 그래서 교회가 건강하게 세워지는 것이 가장 중요합니다.

복음을 받은 자에서 전하는 자로, 아파 울던 자에서 치유하는 자가 되는 것, 그리고 여기 인천에서 평양으로, 평양에서 열방으로 나가가는 것이 저희 교회의 비전입니다. 나중에 알고 보니 여기 인천 지역이 전쟁 당시 황해도 분들이 정말 많이 이주한 지역이라고 합니다. 고향을 그리며 고향 가까운 곳에 터를 잡은 것이지요. 이런 면에서 보면 인천도 분단의 아픔이 있는 땅이 아닐까 싶습니다. 그래서 이곳에서부터 복음을 통한 치유가 일어나고 북한과 열방을 향해 나아가는 비전을 그리고 있습니다. 그러면서 때마다 하나님이 원하시는 것을 분별하고 찾고 순종하고자 합니다.

지면을 통해 김권능 목사님과의 인터뷰 내용을 3회에 걸쳐 나누었습니다. 개인의 인생 가운데서 역사하신 하나님에 대한 간증 뿐 아니라 복음의 능력과 북한과 한국교회를 향한 하나님의 마음과 비전을 다시금 생각해보는 귀한 시간이었습니다. 귀한 메시지를 나누어주신 목사님께 감사드리며 이번 인터뷰가 독자님들의 신앙과 북한을 위한 기도에 도움이 되셨길 바랍니다. (끝)

한국 정부, 유엔 북한인권결의안에 공동제안국 참여

정부가 북한의 인권 상황에 문제를 제기하는 유엔총회 북한인권결의안에 참여했다. 11월 12일 공개된 유엔총회 제3위원회 인권결의안에 한국이 공동제안국으로 이름을 올렸다. 이재명 정부 출범 후 처음 상정된 올해 인권결의안에는 대북 관여를 중시하는 정부 기조를 고려할 때 전임 정부와 다르게 접근할 수 있다는 관측이 제기됐으나 계속 동참한 것이다. 북한이 결의안에 지속해서 반발해 온 점을 고려해 공동제안국 참여에 신중해야 한다는 정부 일각의 기류도 있었던 것으로 전해졌지만, 보편적 가치인 인권문제이니 원칙적으로 임해야 한다는 의견이 힘을 얻은 것으로 보인다.

올해 결의안 초안은 북한의 심각한 인권 상황에 우려를 표하면서 특별히 북한의 '두 국가론'이 가져올 상황에 대한 우려를 담은 것이다. 또 외교적 노력을 장려하고 남북 대화를 포함한 대화와 참여의 중요성을 강조했다.

북한인권결의안은 제3위원회를 거쳐 내달 중 유엔총회 본회의에 상정되고 여기서 최종 채택이 결정된다. 유엔총회는 2005년부터 지난해까지 20년 연속 북한인권결의를 채택해왔다. (참고: 연합뉴스, 11월 12일)

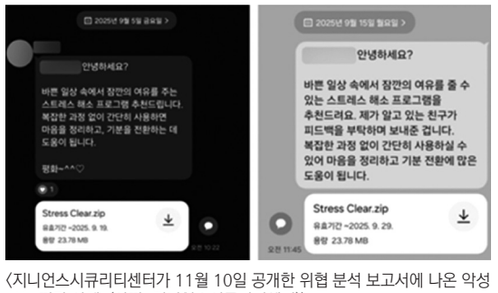
북한선교활동 중 북한에 납치된 장문석 집사 석방

오랜 기간 북한선교 최전선에서 북한 성도들을 돕던 중 북한 당국에 의해 납치된 장문석 집사가 석방되어 11월 귀환했다.

장문석 집사는 중국 길림성 백산시에서 나서 자란 조선족으로 장백현에 위치한 장백교회의 집사로 활동했다. 장백현은 북한 양강도 혜산시와 압록강을 사이에 두고 마주한 도시로 총 인구 73,300명 중 12,200여명이 조선족인 조선족 자치현이다. 장백의 시내에 위치한 장백교회는 1991년 조선족들에 의해 설립되어 한충렬 목사가 담임을 맡은 1990년대 후반 주일 출석 인원 600명의 교회로 성장했다. 교회가 한창 성장 가도를 달리던 1996년과 1997년 수많은 탈북자가 장백으로 쏟아져 나왔다. 장백 세관 근무자에 따르면 2년간 하루 평균 200명가량의 탈북자가 장백 세관을 통해 북송되었다. 이러한 상황에서 한충렬 목사는 장백교회 내 훈련된 집사들을 통해 탈북자와 월경자들에 대한 선교를 본격적으로 시작했다. 이때 장문석 집사도 한충렬 목사를 돕기 시작하여 장백교회의 북한선교에 있어 중책을 감당하는 사역자로 성장했다. 2010년을 전후하여 한충렬 목사와 장문석 집사를 비롯한 장백교회의 북한선교 사역자들에 대해 북한 당국이 테러를 감행할 것이라는 소문이 장백 시내에 파다하게 퍼졌지만, 한충렬 목사와 동역자들은 이에 굴하지 않고 북한선교를 지속했다.

2014년 11월 1일 북한에서 장백을 방문한 성도를 만나러 집을 나간 장문석 집사는 북한에서 파견된 인원에 의해 납치되었고 한충렬 목사 역시 다음해인 1년 반이 지난 2016년 4월 30일 북한에서 보낸 인원에 의해 피살되었다. 장문석 집사의 가족들에 의해 장문석 집사의 15년 구형 소식이 알려졌고 북한선교 현장에서는 이따금 장문석 집사의 생존 소식이 전해지곤 했다. 북한 정권의 구형에 따르면 장문석 집사는 2029년 석방될 예정이었으나 예정보다 4년 빠른 석방이 이루어졌다. 석방 후 길림성 장백현으로 돌아온 장문석 집사는 육신적, 정신적으로 많이 지친 상태로 돌아온 것으로 전해졌으며 가족들과 함께 회복 중인 것으로 알려졌다.

북한 해킹조직, 스마트폰·PC·카톡 장악… 사이버 공격 정황 첫 발견



〈지니언스시큐리티센터가 11월 10일 공개한 위협 분석 보고서에 나온 악성코드 전파 사례. (사진=지니언스시큐리티센터)〉

북한 배후 해킹 조직이 안드로이드 스마트폰과 PC를 원격 조종해 주요 데이터를 통째로 삭제하는 사이버 공격을 한 정황이 처음 발견됐다.

11월 10일 정보보안기업 지니언스 시큐리티 센터는 보고서의 위협 분석 보고서에 따르면, 지난 9월 북한 해커가 국내 심리 상담사와 북한 인권 운동가의 스마트폰을 해킹하고 위장한 악성 파일을 유포했다.

카카오톡 메시지를 통한 악성코드 유포는 전형적인 사회공학 기반 북한발 해킹 공격이지만, 이번 사건에서는 피해자의 스마트폰, PC 등에 침투한 뒤 장기간 잠복하며 구글 및 국내 주요 정보기술(IT) 서비스 계정 정보 등을 탈취하고 스마트폰을 원격 초기화하는 동시에 악성코드를 유포하는 등 여러 수법을 결합한 전략을 사용했다. 이 보고서는 이번 사건이 "기존 북한발 해킹 공격에서 전례가 없었다"며 "북한의 사이버 공격 전술이 사람들의 일상으로 파고드는 실질적 파괴 단계로 고도화되고 있음을 보여준다"고 우려했다. (참고: 중앙일보, 11월 10일)

북한, 10월과 11월 연달아 동해안으로 탄도 미사일 발사

북한이 10월 22일 오전 8시 10분경, 황해북도 중화 일대에서 동해상으로 단거리 탄도미사일(SRBM) 수 발을 발사했다. 해당 미사일들은 약 350㎞를 비행했다. 이날 도발은 APEC 정상회의(10/31~11/1, 경주) 개최를 열흘 앞둔 시점이었고, 미·중·일 주요 정상들이 방한하는 가운데 북한이 존재감을 강조하려는 의도가 깔린 '무력시위'라는 평가가 나온다. 특히 이번 미사일은 내륙을 관통해 동해로 향했는데, 이는 내륙 비행의 위험을 감수하면서도 유도 정확성을 과시하려는 계산된 행보로 분석된다.

뒤이어 북한은 11월 7일 낮 12시 35분경 평안북도 대관 일대에서 동해상으로 또다시 단거리 탄도미사일(SRBM)을 발사했다. 발사체는 약 700㎞를 비행했으며, KN-23 계열로 추정되는데, '화성-11마' HGV(극초음속 활공체)일 가능성도 제기된다. 이 도발은 이재명 정부 출범 이후 두 번째로, 지난 10월 22일 도발 이후 약 16일 만에 재차 감행된 것이다. 이번 도발은 최근 미국 정부가 잇달아 시행한 대북제재 조치, 한미연합훈련 및 항모 전개와 연례 한미안보협의회의(SCM)등에 대한 반발성으로 분석된다. (참고: 언론보도 종합)

북한, 한국 핵잠수함 보유 승인 비난… "핵도미노 초래할 것"

11월 18일, 북한은 한국의 핵추진 잠수함(SSN) 보유 승인과 우라늄 농축 및 재처리 권한 확보 움직임에 대해 강력히 비난했다. 조선중앙통신 논평에서 북한은 이를 미국의 "대결 기도 공식화"로 규정하고, "핵 도미노 현상 초래", "핵통제 붕괴", "자체 핵무장 포석" 가능성을 언급하며 위협을 예고했다. 해당 논평은 3,800여 자 분량으로, 트럼프나 이재명 대통령 언급은 생략해 수위를 조절한 방식으로 보인다. 정부는 즉각 "한국 핵잠수함 추진은 대북적대와 무관하다"는 입장을 내며, "남북 긴장 완화와 신뢰 회복 노력은 계속할 것"이라고 대응했습니다. 북한의 논평은 한미동맹 강화에 대한 반발과 함께, 자국 핵무기의 정당성도 의도적으로 부각한 것으로 평가된다. (참고:언론보도 종합)

1 북한의 기독교 박해 중단을 위해 기도합시다. 하나님의 은혜로 고 한충렬 목사님과 함께 사역하시던 장백의 장문석 집사님께서 12년 만에 풀려나셔서 중국으로 귀환하신 기쁜 소식이 있었습니다. 그렇지만 여전히 김정욱(2013), 김국기(2014), 최춘길(2014) 선교사님을 비롯해 탈북민 출신 김원호(2016), 함진우(2016), 고현철(2016)씨 등이 여전히 억류 중입니다. 거기에 더해 북한은 강제 북송된 탈북 신자들을 정치범 수용소에 수감하고 있습니다. 북한의 기독교 박해가 하루속히 중단되도록, 그리고 하나님을 대적하는 악한 죄에서 회개하고 돌이키도록 기도합시다. 또한 갇혀있거나 추방당한 성도들과 그 가족들의 생존과 신앙을 위해서, 억류되신 선교사님들을 위해서 기도합시다.

2 북한의 사이버 위협 문제를 놓고 기도합시다. 북한은 세계 곳곳에서 사이버 범죄 활동을 적극적으로 벌이고 있습니다. 사상 최대 규모를 기록하고 있는 암호화폐 해킹을 비롯해 방산기술 탈취, 각종 테러 활동, 더 나아가 교회와 성도들을 향한 공격까지 확대되고 있습니다. 특히 북한의 사이버 공격은 북한 선교 사역자나 기관뿐 아니라 일반 교회에도 영향을 미치고 있으며, 그 방식 또한 무차별적인 공격이 아니라 신뢰할 만한 직분자로 속여 신뢰를 쌓는 등 한국 교회의 문화를 잘 이해한 교묘한 형태로 발전하고 있어 더욱 주의가 필요합니다. 북한의 사이버 범죄 활동이 약화할 수 있도록 기도합시다. 또한 한국 교회가 보안에 더욱 주의를 기울이는 동시에 북한의 위협을 북한을 향한 선교적 관심과 참여의 계기로 삼을 수 있도록 기도합시다.

3 한반도의 평화를 위해 기도합시다. 북한은 9월 3일 중국의 전승절 80주년 기념행사에서 중국, 러시아와의 협력 관계를 과시하였고, 10월 10일 당 창건 80주년 기념행사를 통해서 대립적인 국제 정세 속에서 높아진 자신의 위상을 과시했습니다. 북한은 국제사회의 갈등과 분쟁 속에서 자신의 전략적 가치를 높이고, 이를 통해 핵 보유와 경제난을 해결하겠다는 전략에 따라 한반도 긴장 조성을 위해 남한을 적대국으로 지목하고 있습니다. 이러한 북한의 전략이 성공하지 못하도록 기도합시다. 한반도가 북한이 말하는 대결의 장이 아닌 평화의 무대가 되도록, 그리하여 북한의 논리가 힘을 잃고 오히려 평화와 통일로의 진전이 이루어질 수 있도록 기도합시다.

4 해외 북한 선교 현장을 위해서 기도합시다. 북·중·러 3국의 협력 강화가 선교 현장에 어떤 영향을 미칠지 주목됩니다. 복잡한 외교 상황이 선교 현장의 위기를 불러올 위험도 있지만, 북한과 외부 세계와의 교류 확대로 새로운 선교의 기회가 열릴 가능성도 있습니다. 한반도를 둘러싼 국가 간 대결 구도가 심화하지 않고 그로 인해 선교사들의 체류와 활동에 어려움이 생기지 않도록 기도합시다. 또한 북한과 주변국 간의 교류 확대가 더 많은 북한 출신 영혼들과의 접촉점이 확대되는 기회가 될 수 있도록 기도합시다. 일선의 선교사님들과 현장 사역자들이 안전하게 주어진 상황에 지혜롭게 대응할 수 있도록 하나님의 인도하심이 함께하길 구합시다.

5 북한 주민들을 위해 기도합시다. 급등한 북한의 환율과 물가가 안정을 찾지 못하고 있습니다. 이런 가운데 북방의 매서운 추위가 주민들의 일상을 어렵게 만들고 있습니다. 선교 현장에서는 경제적 어려움에 시달리는 북한 주민들의 소식이 계속 전해지고 있는데, 특히 지방의 소외 지역의 상황이 어렵습니다. 심해지는 빈부격차 속에서 고통받는 북한 주민들을 위해, 특별히 빈곤층과

사회적 약자들의 겨울나기와 생존을 위해 기도합시다. 덧붙여 북한 주민들에게 육적인 필요와 함께 영적인 생명이 함께 공급될 수 있도록, 이를 위한 사역의 문이 더욱 활짝 열리도록 기도합시다.

6 북한의 인권 상황이 개선될 수 있도록 기도합시다. 9월 4일 유엔 북한인권조사위원회(COI) 보고서 채택 10주년을 맞아 업데이트된 보고서를 발표하였습니다. 해당 보고서는 북한 내 전반적인 인권 상황은 2014년 이후 개선되지 않았고 오히려 악화한 부분이 많다고 종합 평가하였습니다. 정치범 수용소 운영이나 종교의 자유 제한, 여전한 성분에 따른 차별 및 납북 이산가족 상봉 중단 등이 여전한 가운데, 주민 생활을 억압하는 각종 사상 문화 통제법이 제정되고, 이를 근거로 사형과 공개 처형이 이루어지면서 주민들의 생명권과 정보접근권 및 표현의 자유가 더욱 심각하게 침해되었다고 평가한 것입니다. 북한 주민들을 향한 억압이 끊어지고 주민들이 정당한 권리를 누릴 수 있도록 기도합시다. 북한 당국이 체제 유지를 위한 통제 일변도의 정책에서 벗어나 진정한 '이민위천'의 길로 나아갈 수 있도록 기도합시다.

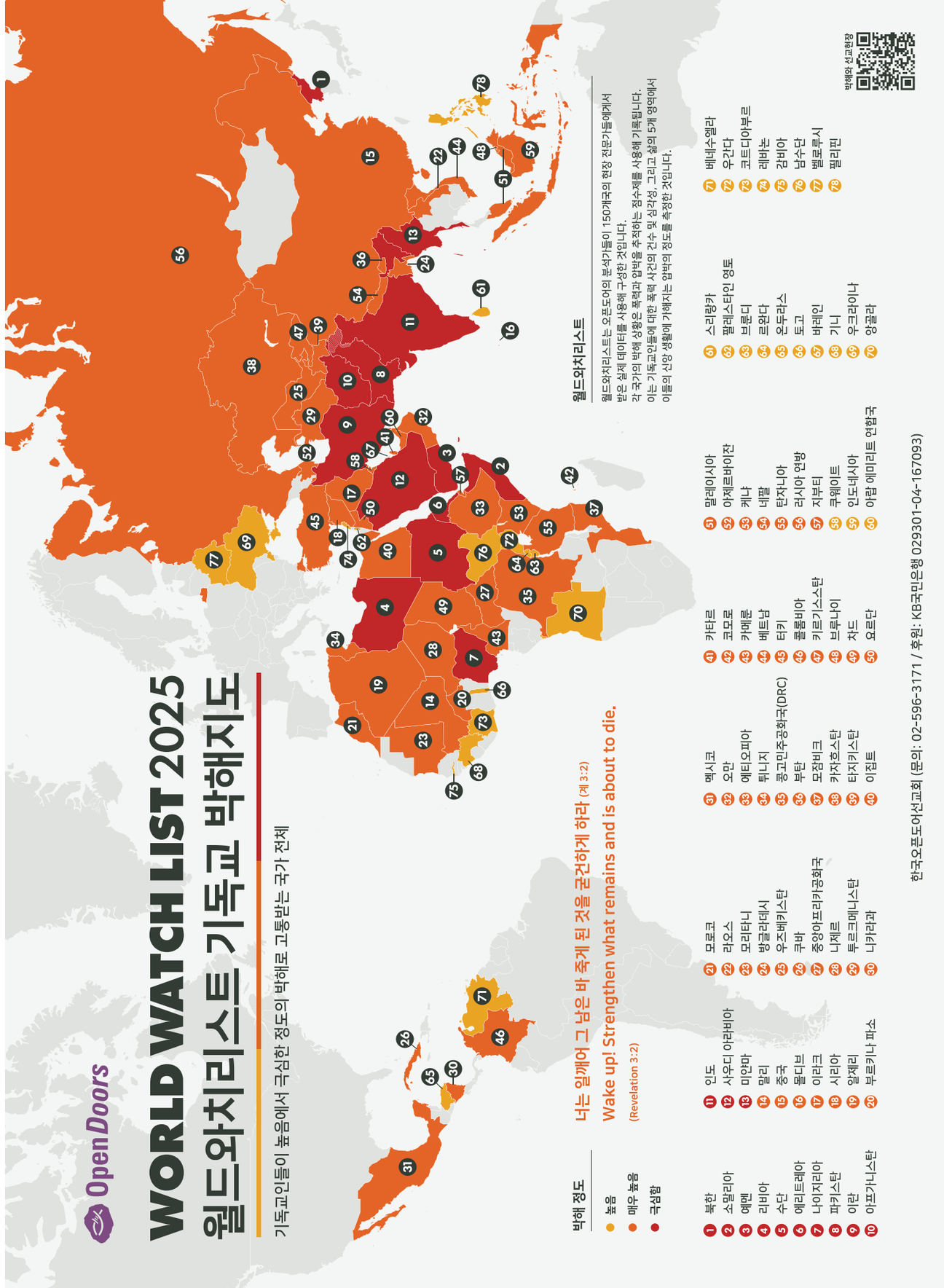
7 해외 북한 노동자를 위해 기도합시다. 24년 러시아로 입국한 북한 주민이 1만 3천 명으로 전년 대비 12배로 폭증한 것으로 집계되었습니다. 25년에는 그보다도 더 많은 북한 사람이 노동자로 파견되고 있는 것으로 보입니다. 중국으로의 북한 노동자 파견도 활발하게 이루어지고 있습니다. 중국의 한 노무 기업이 북한 인력 알선을 선전하는 모습이 포착되기도 했습니다. 북한 밖을 경험하게 될 북한 노동자들이 바깥세상에 대한 경험을 통해 새로운 시야가 열리고, 더 나아가 복음의 기회를 얻을 수 있길 바랍니다. 이들을 향한 창의적인 선교의 기회가 개발될 수 있도록 기도합시다. 북한 사람들과 접촉할 세계 각 지역 교회와 선교사들이 안전에 유의하는 가운데 지혜롭고 창의적인 방법으로 이들에게 그리스도의 사랑을 전할 수 있도록 기도합시다.

8 선교 현장의 기도 제목으로 기도를 부탁드립니다. 악화하고 있는 제3국 북한 선교 환경을 위해 기도합시다. 중국 당국은 지난 5월 1일부터 외국인의 종교 활동을 전면적으로 규제하는 새로운 법률을 시행했습니다. 또한 최근 미등록 가정교회에 대한 대규모 처벌 사건이 발생했는데, 그 내용이 온라인에서 이루어진 종교 활동에 대한 처벌로 알려져 온라인 선교 사역에 비상 경고가 울린 상황입니다. 러시아에서는 2024년 초 탈북자 사역을 하던 백 모 선교사님이 체포되어 현재까지 구금 중입니다. 2010년대 중반 이후 선교 환경이 급격히 악화하면서 많은 선교사가 현장을 떠났고, 아직 회복되지 못하고 있습니다. 선교사들이 어려운 상황 속에서도 생존하며 창의적인 방법을 개발해 사역을 이어갈 수 있도록 기도해 주십시오.

서울시 동작 우체국 사서함 56호 우편번호 07056
* TEL 02-596-3171
* Home Page : www.opendoors.or.kr
* E-mail : info@opendoors.or.kr

▣ 후원계좌 (북한선교)
국민은행 (한국오픈도어선교회)
029301-04-169183

북한월간개발소식 / 등록일 : 2010년 9월 27일 / 등록번호 : 성북, 라 00067 / 발행년월일 : 2025년 11월 28일



Mission Bible College

선교사들이 개발한 'ABC성경대학' 교재

- 셀프 성경 공부 교재
- 교회 소그룹 교재
- 교육 자료가 부족한 해외 선교 현장

본 교재는 국내 교회 및 해외 선교현장에서 성도들이 성경과 신학을 어렵지 않고 체계적으로 배울 수 있도록 현장에서 수년간 사역한 선교사들이 선교 경험을 바탕으로 개발되고 있습니다.

성경을 깊이 있게 공부하고 싶지만, 어디서부터 시작해야 할지 고민하는 평신도,
각종 이단과 불건전한 신학의 홍수 속에서 성경으로 균형잡힌 성도들을 세워가기를 원하는 교회,
평신도 리더를 길러내고자 하지만 교육자료가 부족한 선교현장에 적극 추천합니다.

ABC성경대학(Asia Mission Research Center – Bible College) 교재의 특징

1. 성도들이 복음의 기초에서 한 단계 더 나아가 성경을 깊이 있게 연구하고 리더로 도약하도록 돕습니다.
2. 개인 및 소그룹에서 활용할 수 있도록 본문마다 질문, 묵상, 적용에 중점을 두고 집필했습니다.
3. 성경 해석 참고 도서가 부족한 선교 현장에서 한 권의 책으로 본문 내용을 충분히 이해할 수 있도록 집필했습니다.

AMRC 바이블 칼리지 교재는 기본과정, 성경연구과정, 성경신학과정, 일반신학과정 총 40개 과목을 개발하고 있습니다. 현재 영어, 중국어, 네팔어, 러시아어, 인도네시아어로 번역하여 현지에서 활용되고 있습니다. 그중 사도신경, 주기도문, 십계명은 CLC 출판사를 통해서 출간하였습니다.

※ 사도신경, 주기도문, 십계명은 알라딘, 교보문고, 예스24 등 온라인에서 판매중입니다.
(인터넷 검색창에 CLC사도신경, CLC주기도문, CLC십계명을 검색해 보세요.)