# 2019 한국인터넷거버넌스포럼(KrIGF) 워크샵 보고서

작성자 : 김경곤(고려대학교)

| 세션명 | 워크샵2. 인공지능을 활용한 사이버 위협과 대응 | | | |
|---|---|---|---|---|
| 일시 | 2019.7.5.(금) 11:00~12:30 | | 장소 | 세종대학교 컨벤션센터 |
| 참석자 | 사회 | 최은창 (Fellow) | 발제 | 김경곤 (고려대학교, 교수) |
| | 패널 | 오주형 (KISA, 보안기술확산팀장) | | 이현정 (코스콤, 정보보안팀 과장) |
| | | 김경호 (S-Oil, 정보보안팀 차장) | | |
| | | | | |
| 플로어 | 약 30명 참여 | | | |

| | |
|---|---|
| 제안내용 | 인공지능이라는 단어는 오래전부터 연구 분야에서 많이 사용되어 왔으나, 일반인들에게 가장 크게 다가온 것은 바둑 고수 이세돌과 인공지능 컴퓨터인 알파고의 대결일 것입니다. 이후 인공지능이 일반인들에게 크게 다가왔고, 4차산업혁명이라는 거대한 흐름을 통해 더욱더 인공지능이 핵심적인 요소로 자리잡았습니다. 이제 모든 산업분야에서 인공지능을 외치고 있습니다.<br>사이버보안 분야도 예외는 아닙니다. 매년 수만개 이상의 악성코드가 사이버 공간을 괴롭히고 있고, 악성코드로 인해 사용자들의 개인정보와 금융정보 등이 탈취당하고 있습니다. 더 이상 사람이 악성코드를 하나씩 손수 분석하는 시기는 이제 불가능해졌습니다. 많은 사이버 보안 기업들이 악성코드를 자동으로 분석하고 분류하기 위해 자동화 기법과 인공지능 기법들을 적용하고 있습니다. 악성코드에 대한 인공지능 기반의 분류와 탐지는 거의 95%에 육박할 수준으로 높아졌습니다.<br>한편으로 이러한 인공지능 기술이 보안을 위해서만 사용되지는 않는다는 점입니다. 최근 세계 해킹 컨퍼런스인 블랙햇에서는 인공지능을 이용한 악성코드 공격과 관련된 연구들이 나오고 있습니다. 평소에는 정상적인 소프트웨어로 보이지만, 특정 조건에 부합될 때는 악성코드로 둔갑하여 백신과 같은 보안 소프트웨어의 탐지를 우회하는 것입니다.<br>인공지능은 오래전부터 간헐적으로 이슈화 되었지만, 컴퓨팅 능력이 발달하면서 이제는 우리 삶에 실질적으로 다가오는 시대임은 분명합니다. 이러한 상황에서 사이버보안 분야에서 인공지능의 역할에 대해 다양한 이해관계자들과 논의해보는 시간이 필요합니다.<br><br>• 쟁점 1. 인공지능이 사이버보안에 긍정적인지 아니면 부정적일지?<br>• 쟁점 2. 개인이 인공지능의 위협에 대응할 수 있는 방안이 존재하는가?<br>• 쟁점 3. 인공지능에 대한 거버넌스는 누가 주관해야 하는가? |
| 요약내용 | • 글로벌 인터넷거버넌스 포럼에서도 인공지능과 사이버보안 두 주제가 워크샵에서 언급되고 있음.<br>• 산업,경제적으로 굉장히 파급이 크고 그리고 또 사회적으로 또 정치적으로도 이 주제가 굉장히 크게 이슈되고 있음.<br>• 중요한 주제에 대해서 적절한 시기에 논의가 되고 있는 것 같음.<br>• 김경곤 교수 발표: 인공지능에 대한 개념, 머신러닝, 딥러닝 차이점에 대한 설명. 최근 인공지능을 활용한 사이버보안 기술과 공격 기술 동향 소개.<br>• 최은창 fellow 발표: 옥스퍼드 대학교 캠브릿지 Malicious AI Report 소개. 인공지능을 악용한 딥페이크 영상 소개. AI의 양날의 칼에 비유하며 유용성과 위험성을 이야기.<br>• 오주형 KISA 팀장 발표: AI의 긍정적인 효과, 그중 하나인 사이버 보안 침해사고 대응에 대한 발표.<br>• 이현정 과장 토론: 금융증권 분야에서 AI를 활용하는 분야가 매우 많음. 시장감시팀, 이상징후 탐지, 로봇 어드바이저, 빅데이터 보안에서도 활용하고 있음.<br>• 김경호 차장: 공격자와 방어자 입장에서 인공지능을 사례를 바탕으로 설명. |
| 논의 세부 내용 | [김경곤 교수]<br>• 인공지능이 2016년도에 다보스포럼에서 클라우드 회장이 언급으로 전 세계 대중화가 되었고, 2016년도에 이세돌과 알파고 사건이 있으므로 일반인들에게도 크게 다가 왔음.<br>[오주형 팀장]<br>• 앞으로는 전체 사이버 공격 및 위협에 85%가 AI를 활용할 것이라는 언급.<br>[최은창 Fellow 토론 질문]<br>해외 전문가들의 이론은 AI를 통한 사이버 어택 자체가 기존의 패러다임과는 완전히 바뀔 것이라고 예상. AI를 활용한 새로운 위협들의 지속적인 상승 그리고 확장에 대한 모니터링을 하는데 어떻게 생각하고 계신지.<br>[김경곤 교수]<br>인공지능이 보안 쪽과 연관되는 것은 성능, 속도 문제인데, 공격과 방어 측면에서 방어는 공격자들이 더 어렵게, 더 많은 시간이 걸리도록 해서 우리가 당하지 않고 다른 데로 가도록 회피하는 측면이 있음. 인공지능 활용한 공격 트렌드는 앞으로 지속될 트렌드이고 이것은 정말로 시간, 성능 차이의 문제로 연구가 기대되지 않을까 함.<br>[오주형 팀장]<br>개인적으로 인공지능이 사이버보안과 관련해서 특별히 다를 것이 없다고 생각. 공격에 AI를 쓴다는 것은 크게 두가지를 정리가 됨. 정확도, 효율성을 향상시킨다는 점에서 아까 말씀하셨던 옥스포드 연구소에서 나온 보고서도 그렇고 타당함. 하지만 AI보다 더 위험한건 모든 것이 연결되는 IoT, 5G시대가 더 위험하지 않을까 생각함. 클라우드가 나오고 나서 인프라 가상 관련해서 해커들이 공격을 하고 있음. AI랑 클라우드를 비교했을 때 뭐가 더 위협적이냐? 저는 클라우드라고 생각을 함. 다시 AI로 돌아와서 말씀을 드리면 AI가 해커들에게 악용될 수 있는 것은 당연한 사실. 모든 신기술이 해커에게 악용될 수 있음. 그런데 우리가 이렇게 호들갑을 떨 정도로 위협적일까에 대해서는 의구심. AI가 적용됐을 때 특별히 다를 게 없다고 생각함.<br>[최은창 Fellow] 누가 공격을 했는지 정말 아는 것이 불가능한 것인지.<br>[이현정 과장]<br>실제 공격을 탐지하는 게 포커싱 되어서 하고 있는데 그것을 머신러닝을 돌려서 한 것인지, 사람이 한 것인지, 일정 패턴이 있으면 잡아낼 수가 있기는 하겠지만 확실하지 않음.<br>[최은창 Fellow] AI 공격으로 한 건지 아닌 것인지 아는 것이 가능한 것인지.<br>[김경호 차장]<br>사이버 시큐리티라는 측면에서 공격자가 AI를 쓰든 다른 것을 쓰든, 과정을 쫓아가면 동일하다고 생각. 패러다임이 기존에 기계가 잘하고 반복적이고 특징을 찾는 것에 대해서 AI가 하는 것이고 최종적으로 공격을 하거나 방어를 하는 것은 사람이 하는 방식으로 패러다임이 변경되지 않을까 생각. |

| | |
|---|---|
| | [플로어 질문]<br>유인태. AI 관련해서 사이버 공격에 관련해서 합의 같은 게 있는 것인지, 위협에 대한 합의가 있는지 궁금.<br>[최은창 fellow]<br>사이버 범죄, 보안, 안보에 대한 개념이 전 세계에 통일된 게 없습니다. 그래서 UN 차원에서도 정부대표들이 모여서 국제법상 사이버에도 적용시킬지 그런 부분을 논의하고 있음. 정치학적으로는 난맥상을 보이고 있음. 국제정치를 보면 회식지대고 그렇기 때문에 사실상 인터넷을 지배하고 있는 힘, 입김이 있는 것. 그런 것을 합의할 때 큰 국가가 아닌 이용자라든지 IT 기업들이 합의하는 게 필요하기 때문에 포럼을 만든 것이라고 답변을 드림.<br>[플로어 질문]<br>한국소비자원에서 근무. 실제적인 AI에 관한 침해인지 구별하기가 쉽지 않다고 하셨는데 총괄하시는 입장에서 침해사건을 대응하는 입장에서 봤을 때 이게 구별되는 사례들이 있었는지.<br>[오주형 KISA 팀장]<br>해킹 과정이 정보수집, 침투, 이런 식으로 이루어져 있는데 단계별로 AI가 적용되는 게 있을 것. 정보수집하는 것들을 사람이 계속 해서 정보를 다 수집하는 것보다는 자동화된 AI를 써서 이렇게 가져온다든지 그런 것들이 대응하는 입장에서는 확인이 어려움.<br>[최은창 Fellow Closing]<br>결국 AI와 AI 싸움이라고 할 수 있는데 그 스케일과 속도, 정확도가 가속화되고 있었던 것 같고 여러 전문가 분들의 말씀을 종합하면 많은 경우의 수를 찾아야 하고 누가 했는지 찾기 어렵기 때문에 어려운 규칙이 상당히 위험한 상황으로 가고 있는 것 같음.<br>크게 보면 AI 거버넌스라는 어떤 규제 테마가 있으며, 그 속에서 영국인들이 말하는 트랜스포멘티브 AI가 있음. 사이버 보안을 위협하는 행동, 전쟁 무기에 사용되는 AI 이런 식의 접근들에서 상당히 우려를 하고 있는 게 맞는 것 같음. |