日刊工業新聞
年月日 18 10 12
ページ 10
NO.

ICT 世界の潮流 PART6 13

AIとサイバーセキュリティー㊤

国家存亡の重要問題

国際社会経済研究所（NECグループ）上席研究員
原田 泉

攻撃側が有利

サイバー空間では次々生み出される未知の攻撃を防御することは困難であり、攻撃側が防御側より圧倒的に有利である。しかし昨今の人工知能（AI）技術の進展で、防御力は強化されている。

AIによりマルウエアの振る舞いや属性に関し、ダークウェブなどで取引されている情報を収集しつつ、リアルタイムで大量の通信量を監視して、攻撃に共通するデータや送信元、接続数などの情報を収集し蓄積する。そしてこれらに機械学習、自然言語処理などの分析を加えることで新たな攻撃の予測と迅速な対策が可能となる。加えて、AIは24時間365日働き続け、作業の自動化で管理者の負担を軽減できる。

データ集め困難

今のところ攻撃に関連したデータの収集は容易でなく、AI自身のだまされやすい特性もあって、AIを誤作動させる内部・外部要因を取り除く課題も存在する。しかし今後、これらの問題を解決しつつ、膨大な量のオープンデータからサイバー攻撃に関連した情報を自動モニタリングで収集し、知的で高速・高精度な攻撃監視が進み、自律学習機能も高度化すれば、さらに防御力が高まるだろう。

サイバー空間はAI対AIの戦いの場になる（イメージ）

他方、AIを利用したサイバー攻撃は攻撃対象の絞込みと特定にも力を発揮し、これまで人が行っていた作業の自動化が進むとみられている。AIは人間のハッカーより、複雑な攻撃をより迅速かつ効果的にでき、犯罪者が攻撃をカスタマイズするのを助けることが可能だ。従来は特徴がわずかに異なる亜種のマルウエアを数多く作って検知を回避してきた。今後は機械学習で開発の自動化を進めるなどして、新たなマルウエアがより大量に生み出されるようになると考えられる。

AI対AI

現在のところ犯罪者から見ればまだまだAI利用のコストは高く、本格的な機械学習を用いての新たな攻撃は散見されてはいない。しかし、最近は極めて安価に機械学習アルゴリズムを利用できるシステムが提供され始め、また学習データへのアクセスも容易だ。犯罪者にとってAI利用によるサイバー攻撃のハードルが低くなりつつある。そう遠くない日にサイバー空間は、AI対AIの戦いの場になるだろう。

その戦いの主戦場となるのは、経済面での犯罪者対民間企業・組織はもちろんのこと、国家の安全保障やインテリジェンスの世界となる。サイバーセキュリティー分野でのAI開発は国家の存亡にも大きくかかわる重要問題ともいえる。

軍事面ではすでにAIの利用が進み、その在り方を大きく変えようとしていると聞く。次回はそのAI軍事革命について述べる。

（金曜日に掲載）