平和研所内会議

2013 年 5 月 27 日(月) 開催

テーマ:「サイバー戦争の危機:攻撃の実態と防御」

報告者:大澤 淳(世界平和研究所主任研究員、政策研究大学院大学客員研究員、米国ブルッキングス研究所招聘客員研究員)

概要

現実となった韓国へのサイバー戦争

今年 3 月 20 日午後 2 時、韓国の報道機関や金融機関で、社内インフラネットにつながるサーバーやコンピューターが一斉にダウンした。新韓銀行では、金融取引用のシステムに障害が発生し、支店の窓口業務、ATM、インターネットバンキングが約 2 時間に渡って停止した。KBS(韓国放送公社)では社内ネットワークが停止した為、報道資料の作成に支障が生じ、MBC(韓国文化放送)では記事の作成や映像の社内配信が困難となった。

事件の原因となったのは各企業の社内ネットワークに広がったマルウェアで、このマルウェアが PC のハードディスクのマスターブートレコードを破壊した上で、ハードディスクを特定の文字列で埋め尽くし、PC やサーバーを動作不能にしていった。最終的に 4 万 8 千台あまりの PC が犠牲となった。

4 月 10 日、韓国政府合同調査チームは、3 月に発生した事件が、北朝鮮工作機関の偵察総局が周到に準備をした上で実行した、サイバーテロであるという中間調査報告を発表した(北朝鮮は否定している)。

この 3 月の韓国へのサイバー攻撃は、朝鮮半島が安全保障の面で緊張し、南北が対立を深める中で発生した事件である。北朝鮮は、昨年 12 月の人工衛星と称するミサイル実験に続いて、2 月に第 3 回目の核実験を行なった。これに対して、国連安全保障理事会は北朝鮮に対する制裁決議(安保理決議 2094)を全会一致で採択している。この制裁決議は、従来中国の反対で要請にとどめていた金融制裁や貨物検査を加盟各国に義務づける厳しいものであり、これに対して北朝鮮は非常に激しく反発し、3 月 8 日に朝鮮戦争の休戦協定を白紙化すると宣言し、朝鮮半島に緊張が奔っていた。そのような最中に、今回のサイバー攻撃が発生したのである。

世界に広がるサイバー戦争のリスク

近年、国際安全保障上の危機が、サイバー上でのホットな戦いに発展する事例が増加している。国際安全保障のつばぜり合いが、サイバー上でのホットな戦いとして浮上してきているのが、ここ直近 5 年のサイバー戦争の実情である。実際に、2007 年にはエストニア、2008 年にはグルジア、2009 年には韓国と米国、2010 年にはイラン、2012 年にはサウジアラビアとカ

© Institute for International Policy Studies 2013

タールにおいて、社会インフラ／企業ネットワークを狙った大規模なサイバー攻撃が発生している。今年に入って発生した韓国の事例は、その典型的な例は韓国であった。

韓国において攻撃に使われたこのマルウェアは、システムに最初に感染する先兵の「ドロッパー」と PC を破壊する本隊の「ワイパー」という二つのモジュールから構成されていた。時限攻撃プログラムも内蔵しているこのマルウェアは、2012 年 8 月にサウジアラビアの国営石油会社サウジアラムコとカタールの国営エネルギー会社ラスガスを攻撃したマルウェア「Shamoon」に非常に良く似た攻撃パターンを持っていた。「Shamoon」による攻撃では、原油生産プラントは攻撃を逃れたものの、社内のコンピューター3 万台が感染し、データーが破壊され、ウェブサイトも数週間に渡り閉鎖された。

昨年の湾岸エネルギー企業へのサイバー攻撃は、イランによるものと分析されており、2010 年にイランのウラン濃縮施設の遠心分離機が「Stuxnet」と名付けられたマルウェアで破壊されたことに対する、米国やイスラエルへの報復と見られている。このように、サイバー戦争はもはや SF やハリウッド映画の世界だけでなく、実際の国際政治における紛争の代替手段としての役割を担うようになってきている。

我が国に迫るサイバー戦争の危機

幸いわが国では社会インフラを停止させるような大規模なサイバー攻撃は発生していないが、沖縄県の尖閣諸島を巡る日中対立が激化する中で、中国のハッカーからウェブサーバー等への攻撃が増加しており、サイバー攻撃のリスクと隣り合わせの危険な状態にある。今後わが国を取り巻く国際安全保障環境が厳しくなれば、韓国のようなサイバー戦争は対岸の火事ではなくなる。また、サイバー戦争のもう一つの側面であるサイバー諜報戦は、既に我が国に対して行われてきており、ますます激しさを増している。

政府へのサイバー攻撃が報道されたのは、2011 年 1 月 21 日の NHK の報道「経済産業省にサイバー攻撃」が皮切りであった。同年 9 月には、読売新聞が防衛産業へのサイバー攻撃を報じた。2011 年は、我が国政府機関へのサイバー攻撃が相次いで明らかになった年であり、10 月には、衆議院のコンピュータ・ネットワークへの攻撃が報道され、サーバー等数十台が攻撃によって感染させられたことが判明した。このような政府機関を狙った標的型攻撃は、すでに 2007 年頃より行われていたと見られるが、2011 年になってようやく被害の様子が報道され、広く世間に知られるようになった。

激化する米中のサイバー情報戦争

米中の間では、長年にわたってサイバー空間において、情報戦争が行なわれてきた。中国から米国に対する最初のサイバー攻撃は、今から 15 年前までさかのぼることが出来る。コソボ紛争中の 1999 年に、米軍はセルビア共和国にある中国大使館を誤爆した。これに対して、中

© Institute for International Policy Studies 2013

国からホワイトハウスのウェブサイトにたいしてサイバー攻撃が仕掛けられたのが、始まりである。

米中間では、主に安全保障上の問題に伴って、サイバー攻撃が行なわれたと言われてきたが、2013 年に入り、中国側から民間企業の情報資産を狙った大規模な攻撃が行なわれていることが、明らかになった。

2013 年 1 月 30 日、米ニューヨーク・タイムズ(NYT)紙は、中国から同社のコンピュータ・ネットワークに 4 ヶ月に渡って攻撃があり、すべての従業員のパスワードが流出したと同紙上で発表した。

攻撃を分析したセキュリティ会社 Mandiant によれば、攻撃の手法は過去に中国人民解放軍が関与していた手法と同様であり、様々な状況証拠から、中国政府がかかわったサイバー攻撃であったと結論付けている。

この NYT 紙の報道以後、報道各社、IT 企業が中国からの攻撃を受けた事を一斉に発表している。1 月 31 日ウォールストリート・ジャーナル紙、2 月 1 日ワシントンポスト紙、Twitter 社、2 月 15 日 Facebook、2 月 19 日 Apple 社。2 月 22 日にはついにマイクロソフト社までもが、不正侵入被害を発表した。また、2 月 21 日にワシントンポスト紙は、政府機関、報道機関、研究機関(シンクタンク)などワシントンのほぼすべての組織が中国からハッカー攻撃を受けていると報道している。

これらの一連の報道を受けて、米国政府はサイバー攻撃に対する対策を急速に進める一方、中国に対する警戒感をあらわにしている。 2 月 12 日にオバマ大統領は一般教書演説でサイバー攻撃に対する危機感をあらわにし、一般教書演説に先立って、サイバー脅威に関する機密情報を民間企業と政府の間で共有し、重要なインフラを防護する、サイバー・セキュリティ強化に関する大統領令に署名を行なった。

このような中国から米国に対するサイバー攻撃は、国家間の安全保障上の問題に発展しつつあり、7 月上旬に行われた米中首脳会談でも、主要な議題として取り上げられている。米国では、大規模なサイバー攻撃の兆候に対して、サイバー兵器による先制攻撃を大統領が認めるサイバー交戦規定(ROE)が策定されつつある。わが国においても、サイバー危機に対応するため、米国のように攻撃元に逆侵入し、相手方の特定や反撃を行う「自衛的なサイバー反撃」の容認を早急に考える必要がある。

以上

© Institute for International Policy Studies 2013