【令和２年度航空研究センターシンポジウム（7 月 17 日実施）：発表 5】

抑止及び対処のための「真に実効的な防衛力の在り方」
－サイバーの観点から－

幹部学校客員研究員
時藤 和夫

１　抑止とは

抑止には拒否的抑止と懲罰的抑止がありますが、サイバー攻撃に関しては、100％の抑止というのはできていません。サイバー攻撃は各地で頻発しており、そういう中で、2020 年、米国のサイバースペース・ソラリウム委員会がサイバー防衛についての報告書を出しました。報告書ではサイバー防衛をレイヤー1 からレイヤー3 までの段階に区分し、レイヤー1 の段階では、平時において行動規範を策定すること、サイバー攻撃の烈度が上がってくるとレイヤー2 の段階で拒否的抑止を強化すること、更に紛争状態に近くなるレイヤー3 の段階で懲罰的抑止が必要になる、とあります。米国にとっても、サイバーの抑止は難しいものであることがわかります。

２　サイバー攻撃の特性

背景となるサイバー攻撃の特性について触れておきたいと思います。これは、「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」にも言及されている内容です。多様性として、国家が関与していると疑われる攻撃でも、ネットを通じて攻撃者を参集して、その背後で操りながら攻撃をしかけてくるやり方などがあり、つまり目的とお金と意思統一ができれば、国家だけでなく個人や組織のような様々な主体であっても高度な攻撃を仕掛けることができてしまうようになること。そして匿名性があるがゆえに攻撃を誰が行ったかの特定が困難であること。例えばなりすましメールを送りつけられた時に、

それがどこから来たメールかを最終的に判断するのはそれを受信した人次第になり、ともすればサイバー攻撃の踏み台などとして利用されてしまう危険性にもつながります。そして、隠密性という、なかなか発見されないという特性は、何年もかかって潜んで増殖やサイバー攻撃に必要な情報の収集などをする、これは何年もの間攻撃が発見されていないということになります。攻撃側の優位性という点では、携帯電話を使えばわかると思いますが、頻繁にソフトウェアのアップデートが行われる中には脆弱性対策も含まれ、その時点では 100%これを排除することはできたとしても、新たな攻撃手法が出てくれば後追いの対策になってしまい、常に攻撃側が優位ということになります。これらの特性は抑止の困難性につながります。すなわち抑止ということで、報復攻撃や防御側の対策強化を行うにしても、防御の困難性に加えて報復のための攻撃源の特定が困難であることからも実際には難しいということになっています。

３　米軍のサイバー抑止政策の変遷

米軍におけるサイバー抑止政策の変遷に関して、どのように変わってきたのか説明します。2008 年から 2011 年にかけて、拒否的抑止を中心に行われました。実際にはサイバー攻撃の監視やサイバー攻撃を受けた際の対処が中心で、これにはどこから攻撃をされたのかの特定が困難であった背景があります。2011 年から 2014 年には拒否的抑止に加えて懲罰的抑止にも言及されるようになり、アトリビューションといわれる、誰がどこから攻撃したのかをある程度、根拠がつかめるようになった背景が考えられます。そして 2014 年からは、懲罰的なことを行ったとしても、サイバー攻撃を 100%防ぐことはできないということから、攻撃を前提に回復力等を強化するレジリエンスという概念が加えられました。

４　ハイブリッド戦への対応

最近の戦い方では、ハイブリッド戦やグレーゾーンでの事態にサイバー攻撃が利用され、情報戦の一環としてサイバー空間が活用されています。抑止力確保のために、どうするべきかについてですが、一つは高信頼組織の更なる強化充実があります。これは、組織として不測の事態を正確に認識できる能力につながり、失敗から学んだり、現場の状況に敏感であったり、あるいは不測事態の予測だけで完全としないこと、専門職を尊重することなどが必要です。次に状況把握能力の強化です。これは、見えないサイバー空間を「見える化」して

いくことです。よく言われていることに COP（Common Operational Picture）があり、航跡シンボルのように状況を把握し理解するには効果的です。サイバーの世界は、仮想な空間でもあるためにシンボルだけでなく、色々な情報も加味して状況を認識する必要もあり、単純にシンボル化することに加えて、他国や（国内の）様々な部署との連携が容易なものにする必要もあるでしょう。

民間セクターとの協力体制強化は必須で、安全保障分野だけにとどまらない協力体制の強化構築も必要になります。ただし、情報の共有の適切な方法については我が国として考えなくてはならないところです。また、サイバー攻撃を防ぐことは不可能との認識によるレジリエンス能力に関しては、防護能力と対処能力のバランスも難しいところだと思います。同盟国等との連携強化に関しては、情報を持っている国との連携をしていく必要があります。

５　時代の変化

次に時代の変化についてですが、非対称な技術的優位性の戦略的価値の減少、つまりハイバリュー・アセットがいくらできたとしても、情報の流れが速いためすぐに戦略的価値が低下してしまう時代になりつつあります。加えて、開発期間の短縮化が可能となりつつあり、AI のように、作って使ってみてフィードバックしてまた作るという修正の繰り返しを行う分野でも時間短縮化の傾向にあります。働き方も変化して来ており、デジタル社会構築に向けた取り組みによって、色々なところで場所を限定しないで働くテレワークやオペレーションが行われつつあります。このような流れの中でサイバー攻撃の影響拡大と複雑に概念化されたサイバー空間を適切に認識する必要性に直面しています。そして皆さんは身近なネットを活用した機器や携帯電話を思い浮かべると、IoT や制御システムなどへの攻撃増加による影響は広がっているのが理解できると思います。変化は迅速で複雑化することは、攻撃源の特定やターゲッティングがしにくくなるという問題点にも繋がります。

６　実効的防衛力へのアプローチ

最後に、実効的防衛力へのアプローチについてです。戦力発揮の変遷をみると、自己完結（Self-contained）から組織的な戦力発揮に適したシステム・オブ・システムズ（System of Systems）、更に柔軟に戦力の運用ができるキル・ウェブ（Kill web）をたどって来ました。現在はモザイク（Mosaic）と呼ばれる再構築に重きを置いた概念に向かって変化の時期に来ています。この概念は米軍で進

んでおり、一つを叩いても逐次、アセットのグループを変えて戦力を再構築して継続運用を可能にするというもので、抑止の一つになっています。その中心にあるのがサイバー能力で、今後はその能力をマルチドメイン・オペレーションやマルチドメイン C2 等の運用においても遺憾なく発揮し、レジリエンス能力を強化した戦力向上を現実のものとしていかなければなりません。