2. 法的概念と効果・要件

2.1. サイバー戦争の意義と概念

2.1.1. サイバー戦争の意義

法的なものとしての概念から検討する場合、サイバー犯罪の定義自体は、問題がすくない。コンピュータのセキュリティ等に対する犯罪であって、犯罪の構成要件に該当する違法・有責な行為ということになる。

その一方で、サイバー戦争、サイバーテロリズムの概念となると、近頃の現象を表現する目的のために使われるのであれば格別、法的な一定の効果を発生させるようになるのには、問題があるように思われる。

法的な定義というものを考えるのであれば、一応、「戦争とは国家間の継続的かつ大規模な武力行使のこと」をいうと定義することができる（行為説）。もっとも、厳密に論じるのであれば、「戦争」というのが法的にどのような効果をもつのかという点について、洗い出すのが有意義である。伝統的な戦争に関する法律（戦争法・Law of armed conflict）は、ユス・アド・ベルム（Jus ad bellum）とユス・イン・ベロ（Jus in bello）にわけて論じられてきた。また、これらの具体的な論点を考える前にサイバー戦争という用語が、大きくわけて二つの態様に用いられていることを事前に認識しておくことは有意義であるように思われる。

2.1.2 サイバー戦争のふたつの態様

サイバー戦争という概念は、国家の関与を前提とする概念から、ゲリラ戦争的な概念まで、概念としては広いものである。そのなかでも、ふたつの態様を考えておくことが有意義と思われる。その一つは、実際の戦闘行為の一環としてなされたりする場合であり、いま一つは、純粋にサイバースペースのみでの一定の政治的意図にもとづく熾烈な継続的・全面的攻撃の場合とである。前者が、グルジア攻撃の類型であり、後者がエストニア攻撃の類型である。

2.2. ユス・アド・ベルム（Jus ad bellum）-戦争の許容性の問題

ユス・アド・ベルムは、戦争を開始することの正当性の問題であるが、その目的は、どのようにして戦争を管理するかということにある。戦争は、法的には、国家に帰属するという意味である。そのような国家に帰属すべき武力行使とはどのようなものかという論点について、考える場合においては、ユス・アド・ベルムの法的論点は、（１）国際連合憲章のパラダイム（２）国家責任－属性のふたつであろう。そして、さらにそれに加えて、証明責任を中心とした事実認定の問題についても見ていくことになる。

（１）国際連合憲章のパラダイム

最初に、国際連合憲章の規定をみて、熾烈かつ全面的なサイバー攻撃の位置づけについて考えることにする。国際連合憲章においては、そのようなサイバー攻撃の位置づけに関

連する記述としては、以下の４つの概念を検討することができる。その４つとは、（イ）武力の行使（同２条４項－use of force）（ロ）平和時（同３９条）（ハ）武力攻撃の発生（同５１条－an armed attack occurs）（ニ）武力による反撃（同５１条－exercise of this right of self-defense）となる。これらの関係について見ていくことにする。

（ア）武力の行使（同２条４項－use of force）の意義

憲章２条４項は、「すべての加盟国は、その国際関係において、武力による威嚇又は武力の行使を、いかなる国の領土保全又は政治的独立に対するものも、また、国際連合の目的と両立しない他のいかなる方法によるものも慎まなければならない。」と定めている。この武力の行使（同２条４項－use of force）の規定は、その原則的禁止を定めるものである。具体的な救済に関するものではなく、禁止をさだめるものである。そして、この原則は、具体的な例外を許容するので、具体的な事案において、一定の判断を引き出すことは直接には、できないことになる。具体的には、国連憲章は、第７章 平和に対する脅威、平和の破壊及び侵略行為に関する行動において、警察機能を有しているのであり、それらが具体的な規範となる。

この条項の範囲についての解釈論的な問題もある。「いかなる国の領土保全又は政治的独立に対するものも」と記載されているが、では、そのような効果を有しない武力の行使については、禁止の効力は及んでいるのかということである。この点については、一般的には、その後の「他のいかなる方法によるものも」というところで禁じられるとされている。

また、ここで、この「武力（Force）－以下、フォースという」の意義について、軍事力（armed　force）に限られるのか、経済的・政治的圧力といった軍事力以外の力もふくむのかという点についての争いがある。この点については、歴史的経緯からいって、政治・経済力を含まないということがいえるとして、果たして、それ以外の力については、これに含まれるのかという点については、なおも議論の余地がある。

ところでサイバー攻撃は、この「フォース」を構成するのかということが問題となる。これは以下の３９条の解釈にも関係するので、以下で論じることにしよう。

(ｲ)平和時について

同憲章第 39 条は、「安全保障理事会は、平和に対する脅威、平和の破壊又は侵略行為の存在を決定し、並びに、国際の平和及び安全を維持し又は回復するために、勧告をし、又は第 41 条及び第 42 条に従っていかなる措置をとるかを決定する。」

このような平和時においても、たとえば、小規模な武力行使などが存在する場合がある。武力行使にもっとも「重大な諸形態」である武力行使と「それほど重大でない諸形態」が存在するというのは、ＩＣＪのニカラグア事件等において論じられている立場である。参考になるきわめて興味深い判決がニカラグア事件（管轄権１８８４年１１月２６日・本案１９８６年6月２７日）、オイルプラットフォーム事件（本案２００３年１１月６日）である。ニカラグア事件（本案）においてＩＣＪは、「武力の行使には、武カ攻撃のようなより重大な形態のものとより重大でない形態のものを区別する必要があるが、友好関係原則宣

言にも、米州機構の決議(一九七二年)にも、両者の場合が含まれている。」としている。そして、実際にアメリカのなした「コントラの武装および訓練は、たしかにニカラグアに対する武力による威嚇または武力の行使を伴う」という判断がなされているのである。

では、一般的な理論としては、どのように考えるべきか、そして、具体的にサイバー攻撃に対して、この一般理論をどのように適用するかということが問題になる。この点については、攻撃による被害が重要であるというのが伝統的な立場である。しかしながら、国際連合の憲章の起草者の意図に忠実な解釈という観点から攻撃の性質が重要であるという考え方が主張されている。この立場について、マイケル・シュミットは、結果というのは、その攻撃の性質ほど重要ではないということがいえる[1]としつつ、攻撃の性質を種々の要素から、分析するというアプローチを提唱している。彼によれば、フォースの分析においては、詳細に論じると以下のようになる。

具体的には、

（イ）甚大さ－Severity

武力攻撃は、他のフォースの形態に比較して、人的被害および財産の破壊を引き起こす。これは、たくさんの人間が被害を被っているのか、また、無形資産の損失がどの程度あるのかという点も考えられる。

（ロ）迅速さ－Immediacy

武力による強制や脅威は、急激に発生するのが通常である。外交手段は、時間がかかるということを意味しているので、対抗措置をとるのに、ながい時間をまてない場合であるかどうかが重要であるということである。

（ハ）直接さ－Directness

これは、一つの行動が一つの結果を導き出すのかどうか、という視点である。一つの行為が、他の中間的結果を導いた上にその組み合わせで、なにか結果をもたらすというのは、結果として直接的ではないということになる。

（ニ）侵略性－Invasiveness

いかなる国の領土保全又は政治的独立に対するものに対して、これは、政府が攻撃対象となっているのかどうかということである。

（ホ）測定可能性－Measurability

これは、被害が、測定可能なのかどうかということである。武力による強制は、容易に測定できる。

（ヘ）適法性の概念－Presumptive legitimacy

戦闘行為中において、国家は、適法に攻撃行為をなしうることになる。その一方で、

---

[1] この解釈は、マイケル・シュミットによると、「行為」という用語が、影響を基準として用語よりも理解しやすいということが影響しているのではないかということである。また、彼によると、情報攻撃は、潜在的に大規模被害を惹起しがちである（disastrous）にもかかわらず、物理的に認識しがたいために、性質に注意をする概念は、十分機能していないのではないかというのである

例えば、非戦闘員に対しては、攻撃行為をなしえないというユス・イン・ベロの法理などがある。もっとも、戦闘行為中において、国家であってもなしえないような行為というのは、存在しており、そのような行為については、適法性の推定は及ばなく、むしろ、武力の行使として認識するさいの一つの契機となることなる[2]。

また、自衛権の行使が許容されるの、明確な敵対意識（Hostilities）が認定される場合ということになる。ちなみに、米国においては、この敵対意識（Hostilities）に関しては、「」と定義されている。

対抗措置とは、被害を被っている国家が違法な行為の中止を求め、あるいは救済を確保するために、武力行使にいたらない範囲で相手国に対してとの措置をいう。広い意味では、それ自体違法な行為による対抗する「復仇」とそれ自身は違法ではない行為により対抗する「報復」とがある。また、具体的な手法によって分類するときには、外交、交渉、インテリジェンス、武力による対抗があるということになろう。

インテリジェンス行為については、米国においては、 US person（アメリカ市民、合衆国に居住する外国人、合衆国企業、実質的に米国人より構成される企業）については、国内法の保護がなされるが、その一方で、ＵＳパーソン以外については、プライバシについて制定法の保護が及ばないとされている。そこでなされる通信にかかるインテリジェンス行為について、その具体的な行為をとりあげ、国際法上、対抗措置として許容されるのか、などについては、今後、さらに研究がすすめられるべきであろう。このなかには、サイバーエスピオナージ（外国等についての容易に得られない情報を取得・分析する行動）サイバーカウンターインテリジェンス（サイバー手段を主たるスパイ手段として用いて、外国の作戦を特定し、侵入し、中立化させる活動）を含むことになる。

このインテリジェンス行為のなかには、それ自身として違法性が問題となるものがある。例えば、外国の政府の保護するコンピュータに侵入して、情報を得たときに、それは、わが国でいえば、不正アクセス禁止法違反にならないのかという問題である。また、外国で、攻撃に利用されているボットネットに対して、そのＣ＆Ｃサーバとボットネット間の通信を改竄等して、ボットネットを武装解除するということも考えられる。これらは、通信を取得し、改竄することによって、通信の秘密との問題も起こりそうであるし、また、業務妨害的な分析も可能になる。

具体的に、サイバースペースに限定された攻撃においては、対抗措置として、愛国的ハッキング等の行為が許容されるのかという問題が存在することになる。もっとも、サイバーインテリジェンスと法的問題については、さらなる調査が必要となる分野と思われる。

---

[2]なお、「責任－Responsibility」という要素を追加することもありうる。

後述するように攻撃者が区別による保護をうけるような場合は、逆に国家責任の問題となる。攻撃者の保護の前提条件をみたすようなことがない場合には、国家責任は問題とは、ならない。

また、限定的な武力行使も対抗措置の一つとなる。この場合、正当防衛等の問題となるので、条件としては、急迫性（imminence)、比例原則、合理的なその他の代替方法が存在しないことが条件となる。

(ウ)「武力攻撃」

同憲章５１条は、「国際連合加盟国に対して武力攻撃が発生した場合には、安全保障理事会が国際の平和及び安全の維持に必要な措置をとるまでの間、個別的又は集団的自衛の固有の権利を害するものではない。」と定めている。

この場合、主として問題となるのは、「武力攻撃(armed attack)」の規定の意味ということになる。この定義については、直接の武力攻撃以外にたとえば、間接侵略もその対象とするような広い解釈も存在するが、一般には、国家の領域的一体性と政治的独立を侵すような現実に発生した武力攻撃にたいしてのみ許されるという説が一般的である。

では、次にこの「国家の領域的一体性と政治的独立を侵すような現実に発生した武力攻撃」という定義にどのような場合が該当するかという点については、一般的に、範囲（どの範囲が含まれているのか)、期間（どの程度の長さ攻撃が持続するのか)、強度（どの程度の強さをもった攻撃であるのか）の３つの観点から判断されるとされている。限定的攻撃にたいしては、限定的な対抗措置が採用されうるにすぎないことになる。具体的には、平和時の問題として論じたところである。

現実に武力紛争もともになされた場合にサイバー的な攻撃もともに行われるということがあれば、それについては、伝統的な武力行使およびサイバー攻撃も（その他の戦争法規にしたがっているかぎりで）国際法的な意味で適法となるであろう。

社会的に問題なのは、サイバー戦争という用語が、そのような実際の物理的な武力行使がない場合に、サイバー攻撃のみで、そのような自衛活動をなしうるのかという論点として使われているということであろうと思われる。法的問題としては、そのような狭義のサイバー戦争であっても、特に、異なるものではなく、上述の攻撃の説質を決定する３要素（範囲、期間、強度）から判断されることになる。なお付随した論点として「国」にたいして、というときには、現実に領土の要素が問題になるのかということがあろう。たとえば、自国の領土に保管さている情報のみを外国がリモートで取得し、結局、人命等に対する脅威は、まったく存在し得ないという場合がある。このような場合については、武力行使と認定はされないものと考えられる。

(エ)武力による反撃について

武力行使があったという判断がなされたとしても、それにたいして反撃がなされる場合は、また、別個の法的な要素(必要性および均衡性要件)が加わる。

この点については、北大西洋条約の解釈としても興味深いところがある。同条約の協議条項（４条）は、締約国が、いずれかの締約国の領土保全、政治的独立又は安全が脅かされているといずれかの締約国が認めたときと定めており、サイバー攻撃単独でも、上記安全が脅かされたときと定められており、適用が可能と考えられる。その一方で、同５条は

「締約国は、そのような武力攻撃（an armed attack）が行われたときは、各締約国が、（略）個別的又は集団的自衛権を行使して、北大西洋地域の安全を回復し及び維持するためにその必要と認める行動（兵力の使用を含む。）を（略）直ちに執ることにより、その攻撃を受けた締約国を援助することに同意する。」と定めている。

サイバー攻撃のみでも、上述の要件をみたすものかということが“Cyber Attacks Against Georgia:' Legal Lessons identified”で、議論されている。しかしながら、この問題は、未解決であるとされている。そして、集団的自衛活動が関連しうるかという標準的な基準も存在しないのである。

（２）国家責任

私人行為が、国家に帰属することがあるか、あれば、どのような場合かというのが、いま一つの問題である。この点については、時代の変遷とともに認識の変化があるということがいえよう。私人の行為が、どのような場合に国家の行為と認識されるかという論点についての従来の判断でもっとも代表的なものは、ニカラグア事件についての国際司法裁判所の事件である。

（追加予定）

しかしながら、９１１事件以降、この点についての認識が変更されているということができるのではないかといわれている。テロリストのトレーニングキャンプの存在を認識していて、それを認容している場合に、それは、もはや国家が、関与しているということになるのではないかという議論がなされる。

ここで興味深いのは、ＮＡＴＯ５条適用の要件のための検討要素である。「軍隊の参加があるか」「国家に対するものかどうかー国家の指揮があるか、国家の支持があるか、　国家が活動していないか」「国際人道法上の暴力行為に該当しているかー損害・破壊、傷害・死亡を引き起こしているか」という要素により集団的自衛権の発動要件を満たす場合があるとされている。

（３）証明責任

法律上の問題については、事実認定は、きわめて重要な問題になる。実務家は、証拠を収集し、評価し、個別の条項に規定されている要件事実に当てはめ、法律効果を考える。戦争か否かという事実認定は、米国においては、戦争の権限という観点から重要な意味をもっている。米国の憲法においては、戦争権限をめぐって大統領と議会が分担をしていることになる。大統領は、軍隊の司令官としての立場があり、議会は、戦争についての宣言をする権限を有している。この点については、War Powers Resolution of 1973 (Pub.L. 93-148)が定めている。そして、国家安全と軍事に関する権限は、国防省（Department of Defense）が権限を有することになる。従って、「武力行使」があったという認識がなされると、国防省が、その問題についての責任を有することになる。これらの権限と責任は、合衆国法典１０編に示されている。従って、武力行使があったかどうかという事実についてそれぞれの立場から事実認定がなされることになる。どのような証拠にもとづいて、ど

のような心証でもって判断をするかという点についてであるが、刑事事件においては、合理的な疑いを超えた証明ということがいわれる。その一方で、民事的には、証拠の優越ということがいわれる。戦争法においては、証明責任の程度が明確に議論されているとは思えないが、上記行為者の行為規範として刑事的なレベルの証明がいらないと考えるべきであろう。また、国際法上、証拠方法については、無制限である。事実認定についての法的な枠組みを確定することができたとしても、実際の事実認定については、困難な問題が存在する。現代においては、古典的な宣戦布告がなされて戦争状態に突入するという戦争を想定することは困難なように思われる。特にサイバー戦争といわれる状況においては、そうである。現実にもエストニアに対する攻撃は、国家の関与が疑われたが、その点については、防衛時においても、組織的な攻撃関与が推測されたが、国家の関与というまでは、いかなかったという事実がある。

（４）戦闘行為の適法化

まず、平和時において、国際法上、違法な行為であっても、武力攻撃時においては、適法なものとされることがある。

（５）国家責任の適用による免責

国際法上、国家責任法理というのがいわれている。一般には、国家は、私人の行為それ自体については直接には国際責任を負わない。もっとも、権限ある国家機関が私人(またはその集団)に対して、統治権にもとづく公的任務の遂行を要請する場合には、その私人の行為はその国家に帰属する。これと、攻撃者の国際犯罪との関係は一つの論点となる。サイバー攻撃が、国家行為として国家に帰属したとする場合、その行為者である私人自体は、個別の行為について、刑事責任を問われることにはならない。この場合、個人に対して、その攻撃に対して、コンピュータセキュリティに対する犯罪を構成するとして訴追がなされたとしても、理屈的には、その攻撃行為が指令にもとづいて国家行為とされれば、その個人は、攻撃が戦争法規に反しないかぎり、個別の刑事処罰をとわれないことになる。もっとも、理論的に、サイバー攻撃における戦争法規がどのようなものを考察しうるかが明確ではないという問題は存在している。

（６）防衛体制についての問題

法的概念と防衛体制についての問題というのは、米国においては、サイバー戦争についての防衛の責任は、DOD（国防省）、一方、それ以外は、その他のＤＨＳ（国土安全保安省）になるということである。これは、米国においても、相互の関連・情報相互の連絡に問題があり、非効率なのではないかといわれているところである。

２．３．　ユス・イン・ベロ(戦争時の法)

ユス・イン・ベロは、「武力紛争」の存在を前提に発動される。その発動の要件としての「武力紛争」にそもそも、サイバー攻撃は該当するのかという問題が前提となる。そして、ユス・イン・ベロは、さらに慣習法の問題と中立の問題とにわけて考察されている。そも

そも、

(1)「武力紛争」の存在

何をもって武力紛争ととらえるのか、また、「武力攻撃」との概念との関係はなにかというのが、この問題となる。基本的な概念については、ユス・アド・ベルムにおいて検討したところである。

（2）慣習法原則（Customary principle）

一般的に、ユス・イン・ベロにおける原則としては、４つのものがあげられている。「区別（無差別攻撃の禁止)」「必要性」「比例原則」「シビラリ」である。

(イ)区別（ discrimination）ー無差別攻撃の禁止

LOAC は、攻撃者に対して、攻撃目標を敵の戦闘員（Combatants）か軍事目標（military objectives）に定め、民間人および民間目標を区別するように求めている。また、その結果、軍人と文民、軍事目標と民用物を区別せずに行う無差別攻撃の禁止が定められている。

また、行為規範からも、この区別を可能にするような規範が定律されている。ゲリラ戦争を例にするとき、ゲリラ戦争は、（１）責任をもつ指揮官によって指令されていること（２）遠くから識別可能な一定の明確な記章（insignia）または印（sign）を身につけていること（３）戦争における法と慣習に従って作戦が遂行されること（４）武器をオープンに携行することが条件となり、ゲリラに対して法的な地位が与えられるとされている。ここで、遠くから識別可能な一定の明確な記章（insignia）または印（sign）を身につけていることや武器を公開で携行することが求められることから、区別の原則が可能となっている。

しかしながら、現実には、この原則に従うことは次第に困難になってきている。これは、軍事作戦が、民間人および民間活動に依存することが大きくなってきているからである。この例として、米国陸軍における認識を紹介することができる。

サイバー戦争ということを考えたときに、この区別原則がはたして現実に行使しうるのかという問題点が発生している。たとえば、攻撃システム間の連絡にマイクロソフト社のソフトウエアが使われていたとしても、マイクロソフト社の工場を攻撃してよいという判断には結びつかないはずである。

また、軍事目標という観点から考えると、戦闘用のパケットの位置づけというのも問題となりそうである。現実の戦闘のアナロジーで考えれば、戦闘行為用のパケットについては、一国の技術力でもって、戦闘用パケットを峻別し、峻別、遮断、転換、報復等を考えることもできそうであるが、そのようなこともあまり可能性はなさそうである。

(ロ) 比例原則（ Proportionality）

次の原則は、比例原則である。これは、軍事的攻撃で得られる利点と比較して、民間人および民間機関に与える随伴してしまう被害が、釣り合わないことを禁止するものである。通常兵器においては、技術の進化によりコラテラルダメージや偶然の傷害は、きわめて減少している。標的の分析と武器および戦術の選択についての相当な注意がおこなわれているのである。

しかしながら、サイバー戦争などの２１世紀型の戦争においては、この比例原則の実現が困難になってくる。軍事と民間の連続性が強くなってきていている。軍事関係の輸送手段を攻撃しようとコンピュータを遮断すると、民間物資の輸送を途絶えさせることにもなるし、天候のサービスを停止させれば、民間にも大きな影響を与える。

(ハ) 必要性（Necessity）

現在の法によれば、行為者は、攻撃によって得られる軍事上の必要なメリットを明かにすることができなければならないとされている。５つの最悪の兵器は、戦争で禁止されている。

(ニ)　Chivalry-背信行為の禁止

背信行為(legal deception)が禁止されている。背信行為とは、交戦国双方が法規を遵守しているという信頼を裏切る意図で武力紛争上保護されるものや地位を装うことをいう。これにたいして軍事的奇計（military deception）は許容される。奇計とは、敵を欺くまたは無謀に行動させることを意図した行為で、戦時謀計ともいう。偽装、おとり、陽動作戦などが例である。

(3)中立性（Neutrality）

サイバー戦争状態に敵対国がなった場合に、第三国の対応の選択肢はどうなのかという問題である。その戦争に参加していない国家が、交戦国にたいして中立の立場をとった場合に、中立国と交戦国との間は、中立法により規律され、中立国は平時と異なる中立義務を交戦国にたいして負うことになる。この伝統的中立義務は、黙認、避止および防止の 3 種の義務により構成されている。

この原則とサイバー関係紛争との関係について考えれば、通信手段における管理行為が、中立性違反として考えられるのではないかという問題について検討する必要がある。モニタリング、監視行為が、中立義務違反とは考えられないものとは思われる。

（4）戦闘員の保護

これをサイバー戦争について考えてみるとき、戦闘員の地位について考えれば、通常戦争においては、通信に従事しているとしても、サイバー攻撃に従事していようとその地位は同様に思われる。その一方で、通常の戦闘行為が存在しない段階で、サイバー攻撃のみに従事しているものに対して戦争犯罪を侵しているとして逮捕等がなされうるのかという問題が発生しうることになる。

３　サイバー戦争の概念の限界

3. 1.　近接概念

サイバー戦争に近接した概念としてサイバーテロリズムおよびサイバー犯罪を考えることができる。サイバーテロリズムとは、「準国家的、秘密のエージェントまたは、個人による情報・コンピュータ・システム、コンピュータプログラム、データに対する計画的な、

政治的な動機による攻撃であり、非戦闘員を対象とする暴力をひきおこすものである。」と定義されている。また、サイバー犯罪とは、「コンピュータ・データ及びコンピュータ・システムの秘密性、完全性及び利用可能性に対する犯罪など」をいう概念である(サイバー犯罪条約第二編第 1 章第 1 条)。

3. 2. サイバーテロリズム

サイバーテロリズムの一応の定義については、前述した。法的には、むしろ、テロリズムがどのように世界的に位置づけられているのかというのは有意義であると思われる。米国においては、いわゆる愛国者法において、合衆国法典 18 巻§2331 は、テロリズムを「暴力および生命を脅かす活動および行為であって、連邦法もしくは州法の刑事法違反であり、かつ、(i)民間人を 脅迫もしくは強要すること(ii)脅迫または強要により政府の政策に影響を与えようとすること または、 (iii) 大量破壊、暗殺、誘拐によって、政府の行為に影響を与えようとする意図があるようにおもえるもの」と定義している。愛国者法自体は、サイバー犯罪との関係では、いままで議論のあるところを整理したという性格が強いものといえ、新規に新しい対応が導入されたという点はあまりないということがある。

英国は、テロリズム法 2000 において、同様の定義がなされているが、コミュニケーションシステムに対する攻撃がテロリズムと認定される可能性が正面から認められている点が興味深いものといえよう。

3.3. サイバー犯罪

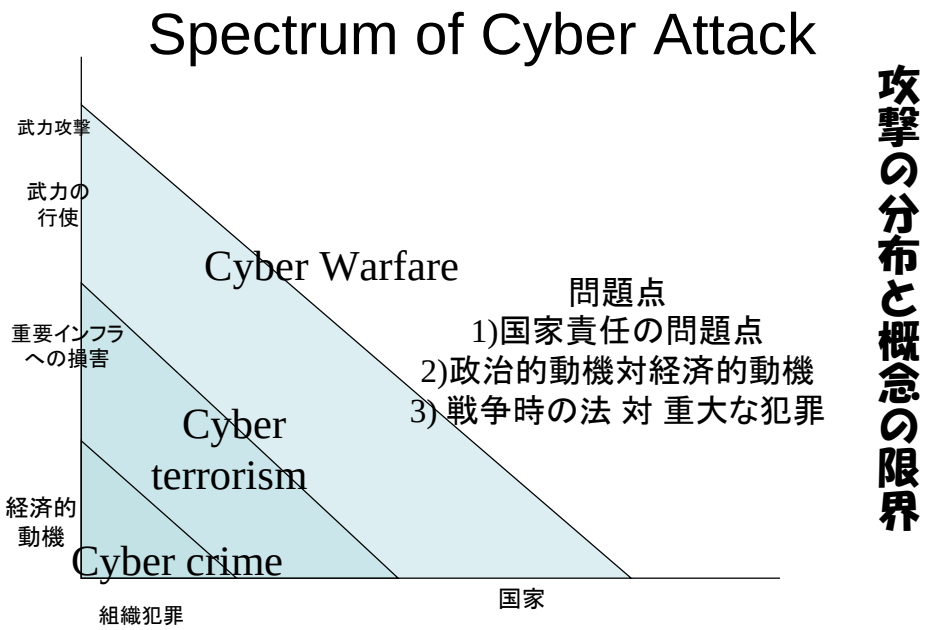
代表的な犯罪として無権限アクセス、無権限傍受、データ妨害、システム妨害、デバイスの濫用などを含む概念であり、コンピュータ関連偽造・同詐欺なども含まれる。

いうまでもなく、個人のみでなす場合もあるし、また、組織犯罪として、大規模なフィッシングなどが行われる場合もある。サイバー犯罪条約については、批准等が、徐々に進んでいるところである。実体法的に整備もなされつつある。もっとも、手続法においては、まだ、外国からの攻撃について、その攻撃者を特定し、刑事罰を課すといういわば伝統的な法執行が有効に機能しておらず、限界を露呈していると評価することができるであろう。

3. 4. 攻撃分布とその概念の限界

（1）攻撃の分布

サイバー戦争、サイバーテロリズム、サイバー犯罪の分布を攻撃力と主体を軸として分布を表したのが次の表となる。



この表は、ある意味で典型的なフォースの分布ということになろう。しかしながら、サイバー戦争についての検討をするとき、むしろ、この典型的な分布と違うところが最大の問題であることが判明している。

（2）概念の限界

（ア）国家とテロリストの限界

この点は、上記のユス・アド・ベルムの議論のうちの国家責任の議論でふれたところであるが、民間人の攻撃を国家の行為とみるかどうかという問題がある。そこで、民間人の行為であっても、国家行為と考えられる理論的な余地があることが明かになった。そうだとして、では、実際に国家は、違法な他国家に対するサイバー攻撃を抑止する立場にあるのか、実際に抑止することが可能であるのかという論点が存在する。

（イ）意図の意義について

実際は、サイバー犯罪が、もはや、テロリズムに対する対応と同様に対処すべき被害を惹起しうるのに、それが、伝統的なテロリズムの概念との関係で、十分な対応ができないでいるのではないかということがいえるものと思われる。上記の定義からも明らかなように、テロリズムの定義においては、政治的・宗教的・イデオロギー的な意図に基づく場合という意図が追加されている。そのような意図にもとづく場合、膨大な被害が惹起されることは、そのとおりであり、テロリズム対応の制度が世界で整備されているのは、まさにそのような根拠にもとづくものであろう。しかしながら、ネットワークでの、多数の者が、特定の指令によるわけでもなく、一定の標的にたいして攻撃がなされる場合も、そのようなテロリズムの被害と比較して、看過しうるものといえるのかという疑問がある。グルジ

アやエストニアの事件は、国家関与というよりも、むしろ、民衆が、インターネットの煽動によって、暴徒化したのではないかという可能性が指摘されている。そうだとすると、あたかも国家と同規模の攻撃を民衆がしかけうるということになったということを意味してしまうのである。

（ウ）ユス・イン・ベロ違反の行為について

ユス・イン・ベロ違反の行為について、どのように考えるべきかという問題がある。すなわち、国家命令のもとに、サイバー攻撃をおこなったとして、それがユス・イン・ベロに違反している場合に、実行者に対して、どのような刑事罰が適用されるのかという問題である。

4 日本における問題

4.1. 戦争に関する規定

まず、わが国において、制定法の問題として考察した場合には、「武力攻撃事態等における我が国の平和と独立並びに国及び国民の安全の確保に関する法律」（武力攻撃事態対処法）の解釈論が問題となる。ここでは、「武力攻撃事態等」という概念が、キーポイントになっている。「武力攻撃事態」とは、武力攻撃が発生した事態又は武力攻撃が発生する明白な危険が切迫していると認められるに至った事態をいい、「武力攻撃予測事態」とは、武力攻撃事態には至っていないが、事態が緊迫し、武力攻撃が予測されるに至った事態をいうとされている（同法２条)。ここで、この武力攻撃自体にサイバー手段のみを使った攻撃が含まれるのかという問題がおこりうる。

もっとも、戦力の行使が可能だといったとして、実際にどのような手法で戦力を行使するのか、たとえば、攻撃用ボットネットなどの利用をすることができるのか、そもそも有効なのかという実際上の問題もある。また、「武力攻撃事態等におけるアメリカ合衆国の軍隊の行動に伴い我が国が実施する措置に関する法律」においては、日米安保条約に従って武力攻撃を排除するために必要なアメリカ合衆国の軍隊の行動が円滑かつ効果的に実施されるための措置が定められているが、サイバー的な防衛について、どのような認識を示すのかという問題は、未解決に思われる。

4.2. テロリズムに関する規定

日本では、いくつかの法令にテロリズムに関連する規定を設けている。具体的には、 「公衆等脅迫目的の犯罪行為のための資金の提供等の処罰に関する法律」においては、第 1 条で、「公衆又は国若しくは地方公共団体若しくは外国政府等（略）を脅迫する目的をもって行われる犯罪行為」と認識しており、また、警察庁組織令 第 39 条 では、国際テロリズム対策課の職務に関してテロリズムについて、「広く恐怖又は不安を抱かせることによりその目的を達成することを意図して行われる政治上その他の主義主張に基づく暴力主義的破壊活動」 として定義されている。ここで、テロリズムとして認識されることは、法的には、その資金の提供等の行為に対して処罰がなされるという実体法上の効果を生むことになる。すでに検討したようにサイバー戦争での論点のうち、行政組織法上の効果について考える

と、テロリズムは、犯罪であり、一般には、警察庁の管轄ということになる。そして、「警護施設もしくはその区域」における「被害を防止するため特別の必要があると認める場合」には、特に自衛隊が出動できるということになっている。では、サイバーテロリズムはどうか。暴力的破壊活動が要件とされており、サイバー手段をもちいての攻撃でそのような結果を導きだすのは、非常に困難なように思われる。もっとも、政治的主義というよりも、ゲリラ的な攻撃（それも抗日ムードのようなもの）について、どのように認識するべきかという論点があるように思われる。

4.3. サイバー犯罪に関する規定

サイバー犯罪条約に対応する犯罪にたいしての刑事処罰としては、ウイルス作成等にたいする犯罪構成要件が不十分であるということは指摘されている。また、不正アクセス禁止法が、きわめて軽い犯罪と認識されている点も十分ではないと考えられる。

文献追加予定