ハイブリッドな脅威通知 JOIN(2018) 16 final

[参考訳]

2018 年 9 月 17 日
明治大学法学部教授
夏　井　高　人

＊＊＊

Joint Communication to the European Parliament, the European Council and the Council: Increasing resilience and bolstering capabilities to address hybrid threats, JOIN(2018) 16 final（Brussels, 13.6.2018）のテキスト（英語版）に基づき、和訳を試みた。そのテキストは、下記の Eur-lex の Web サイトから入手した。

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0016&from=en
[2018 年 9 月 15 日確認]

共同通知 JOIN(2018) 16 final は、情報ネットワーク及び情報システムに対するサイバー攻撃だけではなく、生物化学兵器や放射性物質（CBRN）による攻撃等を含め、EU 及びその構成国に対するハイブリッドな脅威（hybrid threats）への対応策に関する政策文書である。共同通知 JOIN(2018) 16 final は、第 15 次進捗状況報告書 COM(2018) 470 final と相補的な関係にある文書である。

共同通知 JOIN(2018) 16 final は、本文のみで構成されている。この参考訳においては、共同通知 JOIN(2018) 16 final の本文の全文を訳した。

この参考訳においては、原則として直訳とした。直訳のままでは日本語として意味の通らない部分や非常にわかりにくい部分に関しては、やむを得ず意訳とした。

この参考訳は、あくまでも共同通知 JOIN(2018) 16 final の私的な和訳であり、関連分野の研究者のための参考として提供するものである。確定訳ではなく、現時点における検討結果の一部を示すものであるので、今後、必要に応じて改訂・修正が加えられる可能性がある。誤記等があるときは、随時、法と情報雑誌上においてその正誤を公表する。

この参考訳に訳注はない。脚注は、全て原注である。

共同通知 JOIN(2018) 16 final の中で述べられている「Code of Practice on Disinformation」に関する情報は、下記の欧州委員会の Web サイト上で公表されている。

https://ec.europa.eu/digital-single-market/en/news/draft-code-practice-online-disinformation
[2018 年 9 月 16 日確認]

共同通知 JOIN(2018) 16 final の中で述べられている化学兵器、生物兵器、放射線兵器、核兵器（Chemical, Biological, Radiological and Nuclear）による攻撃またはそれらの脅威は、EU 及びその構成国の市民並びに NATO 同盟国の市民の完全な抹殺のような全面的な最終戦争があり得ることを想定するものと考えられるが、現実にそのような事態が発生したときは、（当該行為を実行する主体が死滅してしまっているため）反撃も回復もあり得ないことであることから、そのような最終的局面に至る前の局地戦または市街テロのような事態を想定し、可能な対応策を示していると考えられる。また、このような最終戦は、ハイブリッドの段階を超えた最終的な段階に位置するものである。それは、一般に、古典的な謀略論に見られるような侵攻後に傀儡政権を樹立するための協力者となっていた者や同調者及び扇動者等も含め、敵・味方の区別なく、攻撃対象国の領土上に存在する者を丸ごと全て抹殺して消し去るような極めて単純な全面破壊戦となる。それゆえ、この文脈においては、古典的な謀略論や諜報論だけを前提にものごとを考えることは、極めて危険なことである。

更に、遠い将来のこととしては、このような最終戦の攻撃主体が人間ではない完全自律型の自動システムとなっているような事態も想定しなければならず、そのような事態に至ってしまっている場合には、人間の攻撃者（または侵略者）が存在することを必須の前提とする古典的な謀略論に基づく予測の全てが完全に無意味なものとなることを正確に認識・理解すべきである。

以上のような究極的な最終戦の場合に関しては一応措くとして、一般に、生物化学兵器を用いた局地戦またはテロ攻撃が発生する蓋然性は、核ミサイルによる攻撃の可能性よりも顕著に高いと想定すべきである。そのような事態は、例えば、オリンピックのような大規模イベントにおいて発生する可能性が高いと予測されている。その詳細は、ハイブリッドな脅威と関連する EU の政策文書の中で繰り返し指摘されているとおりである。

そして、EU は、軍のレベル、諜報機関のレベル、警察のレベルだけではなく、生物化学兵器や核攻撃等の際の緊急対応策である EU の市民保護メカニズム（Civil Protection Mechanism）のレベルをも含め、EU 全体を統括し、軍事に関しては NATO とも連携する包括的な危機管理体制を整えつつある（委員会勧告(EU) 2017/1584、共同通知 JOIN(2018) 5 final 参照）。

生物化学兵器に関しては禁止条約が存在する。しかし、一般に、現実には、いかなる条約及び国際協定も、対外的には無意味であり、無力である。特に、究極の状態においては、国際法は存在しない。存在するのは、ナマの実力関係だけである。

これらの事項に関する EU の政策は、現実に発生した攻撃に対する危機管理及び危機対応の段階から、想定（シナリオ）に基づく準備体制の構築及び予防の段階へと進んでいる。その政策が将来どのように進展するかについては、現時点では何とも言えない。

NIS 指令(EU) 2016/1148（OJ L 194, 19.7.2016, p.1-30）に定めるサイバーインシデントのエスカレーションの仕組みと一般個人データ保護規則(EU) 2016/679（GDPR）（OJ L 119, 4.5.2016, p.1-88）に定める個人データの侵害（personal data breach）の通知義務との関係、更に、e プライバシー指令 2002/58/EC（OJ L 201, 31.7.2002, p.37-47）との関係については、委員会通知 COM(2018) 43 final の脚注 7 で触れられているほか、委員会勧告(EU) 2017/1584 でも説明されている。

共同通知 JOIN(2018) 16 final の 3.4 にある「The recent Commission proposals aiming at improving the cross-border gathering of electronic evidence for criminal proceedings」とは、刑事における電子証拠の欧州

提出命令及び欧州保全命令に関する欧州議会及び理事会の規則提案書 COM(2018) 225 final のことを指す。

（この参考訳を作成するに際し考慮した事項）

「the Security Union」は、従前の訳を一括して改め、「安全の欧州連合」と訳すことにした。この場合における「Security」は、「治安」または「保安」または「安全保障」と訳すことも可能ではないかと思われる。

なお、「the Security Union」は、その開始の当初においては、イスラム国（ISIS）の問題を含め、主として宗教的な原理主義に基づく広域のテロ活動に対する対抗策として位置付けられていたものであるが、現時点では、より広範囲に、特定の国家によるサイバー攻撃（State sponsored Cyber attack）や虚偽情報の流布（dissemination of disinformation）による選挙妨害及び治安の悪化を狙うハイブリッド攻撃等を含めるものとして、また、極東地域にみられるような国際的な緊張関係も想定内に入れたものとして、その性格を変化させていると考えられる。

「bolstering」とは、元来は、鉄道の線路を枕木で支えるような場合のことを意味する。共同通知 JOIN(2018) 16 final においては、ハイブリッドな脅威またはハイブリッドな攻撃に対抗するための措置または回復力を維持するための措置を支えるための基礎体力的な下支えのことを意味すると解される。

この参考訳においては、「bolstering」を「支持」と訳すことにした。

「strategic communication」は、ハイブリッドな攻撃としての虚偽情報の流布やキャンペーンに対抗するための反対情報の積極的な出力と伝達のことを意味する。当該虚偽情報を真理であると確信している人々にとっては、政府の権力的な広報活動による思想や言論の弾圧行為として受け止められることであろう。そうでない人々にとっても、その賛否は別として、政府による積極的な広報活動であることには変わりがない。それゆえ、このような方策を実施する場合には、国防、公安または公衆衛生の目的による場合を含め、公共の利益に基づく厳格な正当化事由が存在することを要件とするものと考えられる。

この参考訳においては、「strategic communication」を「戦略的通信」と訳すことにした。

なお、「strategic communication」の定義及び詳細な説明は、ハイブリッドな脅威報告書 JOIN (2017) 30 final の中にある。

EU の機関における「President」は、全て平等に「President」である。それゆえ、この参考訳においては、一般に用いられている訳語を用いることなく、「President」を全て「議長」と訳すという基本方針を維持する。

「EU Playbook」は、「EU 作戦書」と訳すことにした。

「preparedness」は、ハイブリッドな脅威に対する準備体制が整っていることを意味する。

この参考訳においては、単に「準備」と訳すことにした。

共同通知 JOIN(2018) 16 final の脚注 12 は、欠けているので、通知の番号を補って訳すことにした。

共同通知 JOIN(2018) 16 final の 3.3 の囲みの中にある「how to prevent mitigate and respond」は、「how to prevent, mitigate and respond」の誤記であることが明らかであるので、そのように解した上で訳すことにした。

以上のほかは、後掲サイバーセキュリティ通知 JOIN(2017) 450 final の参考訳及び後掲ハイブリッドな脅威報告書 JOIN (2017) 30 final の参考訳の各冒頭部分において述べたとおりである。

（訳出済みの関連法令等及び参考文献）

サイバーセキュリティ通知 JOIN(2017) 450 final の参考訳は、法と情報雑誌 2 巻 12 号 113～147 頁にある。FinTech 通知 COM(2018) 109 final の参考訳は、法と情報雑誌 3 巻 8 号 181～200 頁にある。ハイブリッドな脅威報告書 JOIN (2017) 30 final の参考訳は、法と情報雑誌 2 巻 8 号 91～119 頁にある。委員会勧告(EU) 2017/1584 の参考訳は、法と情報雑誌 3 巻 7 号 293～327 頁にある。委員会通知 COM(2018) 43 final の参考訳は、法と情報雑誌 3 巻 5 号 115～132 頁にある。提案書 COM(2018) 225 final の参考訳は、法と情報雑誌 3 巻 8 号 201～275 頁にある。

NIS 指令(EU) 2016/1148 の参考訳・改訂版は、法と情報雑誌 2 巻 8 号 120～163 頁にある。規則(EU) 2016/679（一般データ保護規則）の参考訳・再訂版は、法と情報雑誌 3 巻 5 号 1～114 頁にある。ENISA 規則(EU) No 526/2013 の参考訳は、法と情報雑誌 3 巻 7 号 263～292 頁にある。

この参考訳を作成するに際しては、上記各参考訳の冒頭部分に掲記の各文献等を参考にした。

＊＊＊

欧州委員会から欧州議会、欧州理事会及び理事会宛共同通知

ハイブリッドな脅威への対処のための回復力及び支持能力の増強

JOIN(2018) 16 final

1. イントロダクション

国家及び国家ではない者によるハイブリッドな活動は、EU 及びその構成国に対し、重大かつ先鋭的な脅威を示し続けている。政府組織への公衆の信頼を損なうことにより、及び、社会の中心的な価値観を攻撃することにより、国々を不安定化しようとする試みは、より一般的なものとなった。我々の社会は、経済と公共サービスを破壊するサイバー攻撃から、敵対的な軍事行動のための標的型の虚偽情報キャンペーンまで、EU 及びその構成国に危害を加えようとする者からの重大な攻撃に直面している。

ハイブリッドなキャンペーンは、相手方を不安定化するための（外交上、軍事上、経済上及び技術上の）在来のツールと戦術及び非在来型のツールと戦術の両者を用い、多面的で、強圧と破壊を結合した手段である。それらは、検知または属性決定を困難にするように設計されており、国家よっても国家ではない者によっても使用可能である。先の 3 月のソールズベリーにおける神経作用薬攻撃[1]は、ハイブリッドな脅威の多様性と現在利用可能な戦術の多角性を更に際立たせている。それに対応して、欧州理事会は、サイバー、戦略的通信及び防諜のような分野において、ハイブリッドな脅威を検知し、防止し、かつ、それに対して対応するための EU 及びその構成国の能力をステップアップする必要性を明確化させた[2]。欧州理事会は、化学兵器、生物兵器、放射線兵器、核兵器と関連する脅威に直面する場合の回復力の必要性について、特に注意を向けている。

非在来型の兵器によって示される脅威は、それらの兵器が発生させ得る損害の潜在的な規模のゆえに、それら自体の類型の中にある。ハイブリッドな脅威を越え、テロリストの脅威をも包含する化学兵器、生物兵器、放射線兵器、核兵器関連の脅威は、国際社会の一般的な懸念の 1 つでもあり[3]、とりわけ、地理的にも国家ではない者にも拡大する、進化するリスクである。

これらの脅威に対する回復力及び支持力を強化することは、主として、構成国の責任に帰する。しかしながら、EU の機関は、国内の努力を強化する助けとなる多数の行動を既に執った。その行動は、とりわけ、北大西洋条約機構（NATO）[4]を含め、他の国際的な関係機関との緊密な共働における作業、及び、緊急対応[5]のような分野における構成国への支援を更に深め得るような作業を含めたものである。

---

[1] ソールズベリーの攻撃に関し、欧州委員会は、3 月 22 日、「ロシア連邦にその責任がある高度の蓋然性があり、かつ、他には可能な説明が存在しないという英国政府の評価結果に同意した」。

[2] 2018 年 3 月の欧州理事会決議

[3] 2016 年 12 月 14 日の国連安全保障理事会決議 S/RES/2325 (2016)の中に含まれている。

[4] ハイブリッドな脅威への対抗は、欧州理事会議長、欧州委員会議長及び北大西洋条約機構事務総長によって 2016 年 7 月にワルシャワにおいて署名された共同宣言書に示されている北大西洋条約機構との協力の 7 つの分野の中の 1 つである。

[5] 2018 年 6 月のシャルルヴォワのサミットの会合において、G7 は、民主主義に対する脅威に対処するため

この共同通知は、この作業を前進させるための欧州理事会の要請に応えるものである。この通知は、2017 年 10 月の化学兵器、生物兵器、放射線兵器、核兵器の行動計画[6]の実装における次のステップを評価し、提出する最新の安全の欧州連合進捗状況報告書[7]、並びに、ハイブリッドな脅威への対抗に関する共同枠組み（欧州連合の対応）[8]の 22 の行動の実装に関する第 2 次進捗状況報告書[9]も含むより広いパッケージの一部である。

2. EU の対応

欧州委員会及び上級代表は、ハイブリッドな脅威並びに化学兵器、生物兵器、放射線兵器及び核兵器関連の脅威に対抗するため、EU の能力を構築し、かつ、構成国を効果的に支援するための一貫性のある努力に投資した。戦略的通信、状況認識、準備及び回復力の強化、及び、危機管理能力の強化のような分野においては、既に、具体的な結果が達成された。

2015 年 3 月の欧州理事会の後に設置された East Stratcom タスクフォースは、外国の情報源からの虚偽情報の発信を予測すること、追跡すること、及び、これと闘うことに関する先兵的な仕事をもつ。そのタスクフォースの専門的な分析及び公開成果物[10]は、ロシアの虚偽情報の影響に関する認識を大きく向上させた。過去 2 年以上にわたり、タスクフォースは、4000 を超える個別の虚偽情報事案を発見したが、その多くは、意図的に欧州を標的とするものであった。East Stratcom の仕事は、東部近隣諸国における守備範囲の増加を伴って、積極的な情報提供の改善にも向けられている。この成功の後、異なる地理的対象をもつ 2 つの別のタスクフォースが設置された（西部バルカンタスクフォース及びアラブ語圏専門の Task Force South）。

状況認識を向上させ、意思決定を支援するために必要な組織体を構築するための重要な手立てが講じられた。2016 年、欧州対外行動局の EU 諜報及び情報センター内に Hybrid Fusion Cell が設置された。Fusion Cell は、ハイブリッドな脅威と関係する異なる利害関係者から、機密情報及びオープンソース情報を受け取り、分析する。今日までに、100 を超える分析評価と報告が行われ、EU の意思決定機関に情報提供するため、EU 内及び構成国内で共有された。戦略的な対話を推進し、ハイブリッドな脅威の調査研究及び分析を実施するために 2017 年 4 月に設置された研究拠点は、現在、そのメンバーを 16 か国[11]に拡大し、EU からの継続的な支援を受けている。

とりわけ、化学兵器、生物兵器、放射線兵器及び核兵器関連の脅威に対する支持の準備及び回復力にも重要な前進があった。過去 6 か月において、化学兵器、生物兵器、放射線兵器及び核兵器と関

の G7 の緊急対応メカニズムを発展させることも合意した：
https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/

6 COM(2017) 610 final.

7 効果的かつ真の安全の欧州連合をめざす第 15 次進捗状況報告書 COM(2018) 470

8 Joint Report on the implementation of the Joint Framework on countering hybrid threats (July 2017-July 2018), JOIN(2018) 14.

9 JOIN(2016) 18 final.

10 http://www.euvsdisinfo.eu/

11 現在の 16 か国中の 14 か国は、EU の構成国である：すなわち、チェコ共和国、デンマーク、エストニア、フィンランド、フランス、イタリア、ドイツ、ラトビア、リトアニア、オランダ、ポーランド、スペイン、スウェーデン、英国である。その創設のための取り組みは、ハイブリッドな脅威への対抗に関する共同枠組みから来ている。拠点は、その協力の枠組み内で、EU 及び北大西洋条約機構からの積極的な支援も受けてきた。

連するセキュリティインシデントの準備、すなわち、化学兵器、生物兵器、放射線兵器及び核兵器の攻撃を防止することを幇助するための能力の検知の面における識別の格差解消において、大きな前進があった。欧州委員会の取り組みにおいて、国内専門家のコンソーシアムは、異なるタイプの化学兵器、生物兵器、放射線兵器及び核兵器関連シナリオのための装備の検知における格差の分析を実施した。格差の分析の報告書は、構成国が、情報を受けた上での検知戦略の決定をできるようにするため、及び、発見された格差に対処するための運用上の措置を講ずることができるようにするため、構成国間で共有された。

この作業は、進捗の度合いを試すための演習を介して後方支援された。北大西洋条約機構との 2017 年の並行統括演習（PACE17）は、大規模なハイブリッド危機に対する EU の対応能力を詳細に試すことを可能にした。範囲の面においてかつてない規模で、「EU ハイブリッド作戦書」、EU の異なる対応メカニズム、及び、それらが相互に効率的に連携する能力のみの試験を実施しただけではなく、EU のハイブリッドな脅威への対応をどのように北大西洋条約機構の行動と連携させるかについても試験が実施された。2018 年の演習は、年次で実施するものとして構築するためだけではなく、構成国の危機対応能力を強化するために構成国を支援するためという大望をもって、計画段階にある。

これらの具体的なステップは、EU によって設けられる政策枠組みが、いかに収穫の多いものであるかを示している：過去 2 年間は、EU の作業をガイドし、焦点を絞るための一連の枠組みを示すものであった。

2016 年 4 月の*ハイブリッドな脅威に関する共同枠組み－欧州連合の対応*[12]は、22 の行動分野をもち、**ハイブリッドな脅威**への対抗を助け、EU 及び構成国並びに国際的パートナーの回復力を育成するための全ての政府のアプローチを推進した。共同枠組みの中に定める主要な行動は、状況認識の向上、及び、より良い対応能力をもつ回復力の構築に焦点を当てている。それらは、重要インフラの保護及びサイバーセキュリティの強化のための能力の EU の諜報機関の分析を支持することから、過激主義及び暴力的な排外主義との闘いまでの幅をもっている。共同枠組みの実装に関する第 2 次進捗状況報告書[13]は、この共同通知と並行して採択され、これらの活動に関する具体的な進捗を示し、かつ、ハイブリッドな脅威に対抗するための EU の努力の強化及び深化を確認するものである。

サイバーセキュリティに関し、2018 年 5 月 9 日は、サイバーセキュリティに関する EU 全域の法的な拘束力のある規定の最初のセットであるネットワークシステム及び情報システムの安全性に関する指令を国内法化するための EU の全ての構成国の期限として、重要なランドマークであった。これは、EU のサイバーセキュリティの構造及び能力のための大きな加速を提供する広範で具体的な措置をもつ 2017 年 9 月の*回復力、抑止力及び防衛：EU のための強力なサイバーセキュリティの構築に関する共同通知*[14]に定める、より広い取り組みの重要な一部である。これは、サイバー攻撃に対する EU の回復力の構築の中心にあり、EU のサイバーセキュリティの能力をステップアップさせ；効果的な刑事法上の対応をつくり出し；そして、国際協力を通じて、グローバルな安定性を強化するものである。それは、EU レベルの支援を強化するための Cybersecurity Act の提案[15]を伴うものであり、実装を介して実施される必要のある一連の提案（後述参照）によって後方支援された。

---

[12] JOIN(2016) 18 final.

[13] 第一次実装報告書（2017 年 7 月）に関し：JOIN(2017) 30 final。

[14] JOIN(2017) 450 final.

[15] COM (2017) 477。後掲参照。

虚偽情報は、市民が情報提供を受けた上で判断する能力及び民主的なプロセスに参加する能力を損なうことにより、我々の民主主義に対して危険を及ぼす。インターネットは、市民にとって利用可能なニュースの分量及び種類を莫大に増加させた。しかしながら、新技術は、不信の種を播き、社会的緊張をつくり出すために精密に狙いを定め、未曾有の規模と速度で虚偽情報を広めるためにも利用され得る。*オンライン虚偽情報との闘いに関する欧州委員会通知:欧州のアプローチ*[16]は、とりわけ、異なる利害関係者に対し、とりわけ、オンラインプラットフォームに対してだけではなく、メディア企業に対しても、行動を執ることを要求することにより、虚偽情報の問題への対応における欧州のアプローチを定めた。これらの行動は、透明性の増加;オンラインプラットフォームの信頼性及び説明責任;より安全かつ回復力のある選挙プロセス;教育及びメディアリテラシの育成;品質評価ジャーナリズムの支援;並びに、戦略的通信を介した虚偽情報への対抗を含め、広範な関連分野を包摂している。最初の具体的なステップは、この夏の前に設けられる虚偽情報に関する多角的利害関係者フォーラム及び事実確認者ネットワークによって策定される虚偽情報に関する行動規範を含む。虚偽情報に関する多角的利害関係者フォーラムの、2018 年 7 月に行動規範を採択するために要するステップを合意する最初の会合は、2018 年 5 月に開催された。欧州委員会は、2018 年末までに、問題との闘いにおいて行われた進捗状況を評価し、この分野において追加的な介入が必要であるか否かを判断する。予定されている活動は、East Stratcom タスクフォースの活動と一貫性があり、かつ、補完的なものとなるであろう。

化学兵器、生物兵器、放射線兵器及び核兵器のリスクに関し、欧州委員会の 2017 年の*行動計画*[17]は、EU とその構成国との間の緊密な協力、及び、北大西洋条約機構との間の緊密な協力を介するものを含め、これらの脅威に対する市民及びインフラのより良い防護を狙いとする 23 の実践的な行動及び措置を提案した。テロリズムに対する防御及び回復力を向上させるための安全の欧州連合における措置の一部として、その行動計画は、化学兵器、生物兵器、放射線兵器及び核兵器と関連するリスクが低程度であるようであっても高程度であり、攻撃の時点における影響が持続するという正当化事由を根拠とする予防的なアプローチに従うものであった。その間、ソールズベリー攻撃が発生し、並びに、EU の内外における化学兵器、生物兵器、放射線兵器及び核兵器の使用に対するテロリストの関心及び能力に関する懸念が増大した[18]。これらは、化学兵器、生物兵器、放射線兵器及び核兵器と関連する物質によって示される脅威が現実のものであることを証明することとなった。このことは、行動計画を全面的に実装する緊急の必要性を更に高めるものである。行動計画は、全ハザードアプローチに従い、以下の 4 つの目標に焦点を当てている:すなわち、化学兵器、生物兵器、放射線兵器及び核兵器と関連する物質へのアクセス可能性を削減すること;化学兵器、生物兵器、放射線兵器及び核兵器のセキュリティインシデントへのより堅牢な準備及び対応を確保すること;重要な領域パートナー及び EU の国際的パートナーとの間の化学兵器、生物兵器、放射線兵器及び核兵器のセキュリティにおけるより強力な内部連携及び外部連携を構築すること;そして、化学兵器、生物兵器、放射線兵器及び核兵器の知識を拡大することである。行動計画の実装の具体的な進捗状況に関する詳細な報告は、この共同通知と並行して採択される最新の安全の欧州連合進捗状況報告書の中で提供される。

---

16 COM (2018) 236 final.

17 COM(2017) 610 final.

18 Europol, Terrorism Situation and Trend report (TE-SAT) 2017, p. 16
www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf
OPCW 事務総長の声明も参照:www.globaltimes.cn/content/1044644.shtml

最後に、ハイブリッドな脅威に対抗するための努力の実効性を増加させること、及び、EU の構成国間及び北大西洋条約機構（NATO）の連合国との間の一体性、ハイブリッドな脅威に対する協力関係のメッセージを強化することは、2016 年 7 月のワルシャワ共同宣言[19]の中で示された EU と NATO 間の協力の重要な分野の 1 つとして定義されてきた。協力関係に関する現行の全ての共通提案の 3 分の 1 近くは、ハイブリッドな脅威に焦点を当てている[20]。上述の演習及び「EU 作戦書」[21]は、本年において深化された協力関係の上に構築されている。

3. 進化する脅威への対応をステップアップする

3.1. 状況認識－ハイブリッドな脅威を検知するための能力の向上

ハイブリッドな脅威への対抗及び対応のための努力は、不正なハイブリッド活動及び内外のその発信源を早期に検知し、かつ、しばしば一見すると無関係の出来事の間のあり得る関連性を理解する能力によって支えられなければならない。その目的のために、オープンソースの情報を含め、利用可能な全てのデータの流れを利用することが重要である。

ハイブリッドな脅威の分析に焦点を当てた EU の単一連絡部局として EU Intelligence and Situation Centre 内に設置された Hybrid Fusion Cell は、重要な資産の 1 つであるが、化学兵器、生物兵器、放射線兵器及び核兵器並びに防諜の分野を含め、ハイブリッドな脅威の全てのスペクトラムに対処するために必要となる専門知識を要する。専門知識を拡大することは、これらの特殊な分野におけるより完全な民間情報及び軍事情報を提供することによって、将来の EU の危機対応への支援を増加させ得る。これは、Hybrid Fusion Cell に対する構成国の国内機関の情報活動上の貢献を増加させるための構成国の活動、及び、緊急を要する情報を提供及び処理するための Hybrid Fusion Cell との国内連絡部局を構築する能力を更に拡大するための構成国の活動によって後方支援され得る。もう 1 つのステップは、構成国に対し、潜在的な脅威のより深い分析を可能とするための、EU 諜報及び情報センター（INTCEN）に対する構成国の国内機関の情報活動上の貢献の増加に注意を向けさせることとなるであろう。

将来のステップ

- 上級代表は、化学兵器、生物兵器、放射線兵器及び核兵器に特化した防諜、並びに、サイバー分析のコンポーネントによって、Hybrid Fusion Cell を拡大することになる。構成国は、既存のハイブリッドな脅威及び発生しつつあるハイブリッドな脅威の分析のため、Hybrid Fusion Cell への情報活動上の貢献をステップアップすることの要請を受ける。
- 欧州委員会は、上級代表と連携して、構成国が、異なる部門におけるハイブリッドな脅威の可能性をより良く評価できるようにするための脆弱性指標に関する作業を完了させる。この作業は、ハイブリッドな動向の EU の分析も支援することになる。

[19] Juncker 議長、Tusk 議長及び NATO 事務総長 Stoltenberg によって署名された宣言書は、EU と NATO 間の協力のための現行の基盤を構成する。
[20] 15283/16 and 14802/17.
[21] SWD(2016) 227 final.

3.2. 化学兵器、生物兵器、放射線兵器及び核兵器の脅威に対する行動の強化

2017 年 10 月の化学兵器、生物兵器、放射線兵器及び核兵器のセキュリティリスクに関する行動計画は、EU レベルにおける準備、回復力及び調整のための枠組みを定めている。それが定める行動は、専門知識の蓄積及び共同の能力構築、知識及びベストプラクティスの交換、並びに、運用上の協力のステップアップによって、構成国を支持するための幅広い措置を包含している。構成国及び欧州委員会は、行動計画を緊急事項として全面的に実装するために共に作業する必要がある。加えて、検知能力の格差分析の面において既に行われた進捗状況、並びに、新たに設置された化学兵器、生物兵器、放射線兵器及び核兵器諮問グループにおけるベストプラクティスの交換を基盤として、欧州連合は、発展し続け、進化し続ける脅威に対処するための更なる措置を現時点で講じなければならない。この措置は、とりわけ、化学的な脅威に対して適用される。爆薬前駆物質へのアクセスを禁止するための作業[22]の実例に従い、EU は、ハイリスクな化学物質へのアクセスをより良く監視するため、及び、可能な限り早い段階でそのような物質を検知する能力を最適化するための迅速な運用措置を講ずる必要がある。構成国もまた、例えば、化学兵器、生物兵器、放射線兵器及び核兵器の回復力、並びに、資産及び経路の除染に関し、格差分析を更に実施し、かつ、EU レベルの演習とのマッピングを検討しなければならない。化学兵器、生物兵器、放射線兵器及び核兵器による攻撃の結果に対する準備を整え、それを管理することは、市民保護当局を含め、構成国間における協力と共働の強化を要する。欧州連合の市民保護メカニズムは、準備し、対応するための欧州の集団的な能力を強化することを狙いとするこのプロセスにおいて、重要な部分の役割を果たし得るものである。

国際協力もまた、この作業における重要な要素の 1 つであり、EU は、北大西洋条約機構との波及効果を求めることを含め、地域的な化学兵器、生物兵器、放射線兵器及び核兵器情報センター、並びに、南部及び東部のための自然災害及び人為的災害の防止、準備及び対応計画[23]との連携を基礎とすることができる。

将来のステップ

- EU は、化学兵器に関する EU の可能な特別制裁制度による場合を含め、化学兵器の使用に対する国際的な法令及び基準の尊重を支持するための手段を探究しなければならない。
- 化学兵器、生物兵器、放射線兵器及び核兵器の行動計画を前進させるため、欧州委員会は、2018 年末までに、構成国と共に、以下のステップを完了するための作業を行う:
  - それらへのアクセス可能性を削減するための運用上の行動のための基盤として、特別の脅威を示す化学物質のリストを策定すること;

[22] テロリスト及び犯罪者が活動する空間を閉じるための安全の欧州連合内における作業の一部として、欧州委員会は、手製の爆薬の製造のために濫用され得る爆薬前駆物質へのアクセスを削減するための緻密な行動を執った。2017 年 10 月、欧州委員会は、既存の法令に基づき、爆薬前駆物質の濫用を防止するための迅速な行動を定める勧告(勧告 C(2017) 6950 final)を提示した。それを基礎として、欧州委員会は、2018 年 4 月、爆薬前駆物質のマーケティング及び利用に関する既存の規則 98/2013 を改訂し、強化する提案を採択した(COM(2018) 209 final)。

[23] 東部及び南部の近隣諸国において、地域的な自然災害及び人為的災害の防止、準備及び対応計画に基づき、市民保護の訓練及び演習が行われている。

- ー 前駆物質として使用され得る化学物質からの進化する脅威に対処することに向けて共に作業するため、流通網内の民間関係者との対話を設けること;
- ー 構成国の検知能力のステップアップのための構成国向け運用ガイドを策定することを狙いとして、化学物質の脅威の検知を向上させるための脅威シナリオの見直し及び既存の検知手法の分析を加速させること。

● 構成国は、基本的な治療薬の備蓄、研究所、治療及びその他の能力の目録を設けなければならない。欧州委員会は、構成国と共に、攻撃の場合における構成国のアクセス及び迅速な配備を向上させるため、EU 全域にわたるこれらの備蓄の利用可能性を継続的にマップするための作業を行う。

3.3. 戦略的通信ーー貫性のある情報伝達

情報と虚偽情報とを見分けるための認識を向上させ、一般公衆を教育することは、ハイブリッドな脅威と関連する重要な検討課題である。East Stratcom タスクフォース、EU Hybrid Fusion Cell 及びハイブリッドな脅威に対抗するための欧州研究拠点、並びに、欧州委員会によるそれら以外の努力[24]の経験を基礎として、欧州委員会及び上級代表は、体系的な連携及び既存の組織構造の間の一貫性を確保することにより、EU の戦略的通信の能力を更に開発し、専門化する。これは、虚偽情報に関する通知された安全なオンラインプラットフォームを使用することを含め、EU の他の機関及び構成国に更に拡大されることになる。EU の機関の間、構成国との間、並びに、国際的パートナー及び国際機関との間の戦略的通信に関する協力と共働の改善は、重要なものとなり、また、リアルタイムの危機に対して対応する前の時点における準備及び実務を要する。

選挙期間は、とりわけ、サイバー可能化攻撃の戦略的かつ機微の標的となることが証明され、選挙活動禁止期間、透明性のある選挙資金規則、及び、候補者の平等な取扱いのような、在来の（「オフラインの」）防護措置及び法令のオンラインの回避となることが証明された。これは、電力インフラ及びキャンペーン用 IT システムに対する攻撃、並びに、民主的な選挙に不信を抱き、非合法なものとすることを狙いとする第三国からの政治的な動機による大量オンライン虚偽情報キャンペーン及びサイバー攻撃を含む。これらの進化する脅威への準備及び対応において構成国の認識を向上させるため、EU レベルで、幾つかの作業の擦り合わせが実施されているところである。理事会において、構成国のサイバーセキュリティ当局[25]は、選挙のライフサイクルを通じて選挙技術のサイバーセキュリティに対処するための任意的な運用指針を発行し、共通のベストプラクティスを定める。これは、投票者及び候補者を登録し、投票を集計し、結果を広報するために使用される情報システム及び ICT ソリューション、並びに、選挙結果の正当性と直接に連携する補助システムを含める。

---

[24] 欧州委員会の代表者は、例えば、事実確認及び神話退治の分野においても活動している。幾つかの構成国は、フランスにおける *Les Décodeurs de l'Europe*、イタリアにおける UE Vero Falso、オーストリアにおける公開の EU 神話退治漫画コンペティション、ルーマニアにおける同様の漫画シリーズ、及び、英国代表の Euromyths A-Z のような、地域的に採択されたツールを開発した。そのようなものが更に作成中である。

[25] ネットワークシステム及び情報システムのセキュリティに関する指令に基づいて設置された共同活動グループの後援に基づく。

将来のステップ

- 欧州対外行動局及び欧州委員会は、EU の内外からの虚偽情報に対処するため、及び、敵対的な虚偽情報製品及び外国政府によるハイブリッドな干渉を検知するため、戦略的通信に関するより組織化された協力を構築するためのそれらそれぞれの職務権限の範囲内において、共に作業を行う。
- 欧州委員会は、選挙に対するサイバー可能化の脅威及び虚偽情報の脅威をいかに防止し、緩和し、及び、これに対応するかに関するベストプラクティス及び運用指針を促進するため、民主主義に特化した基本権コロキアムを含め、構成国及び関連利害関係者と共に、この秋に、ハイレベルのイベントを開催する。
- 上級代表及び欧州委員会は、EU の努力が、敵対的な者によって実行される虚偽情報キャンペーンの複雑性に対処するために十分な規模をもつことを確保するため、ツール及び資金の面において、3 つの Stratcom タスクフォースによって実施される作業をより良く支援するための方法を注視する。

3.4. サイバーセキュリティ部門における回復力及び支持力の構築

サイバーセキュリティは、我々の繁栄と安全の両者にとって不可欠の重要性をもつ。我々の日々の生活及び経済は、ますますもってデジタル技術に依存するようなってきているので、我々は、ますますもって脅威に晒されるようになっている。

今日の EU における実効的なサイバーセキュリティは、不十分な投資と不十分な調整によって損なわれている。EU は、現在、サイバーセキュリティにおける技術と配備を高度化させるため、支援措置、より強力な調整及び新たな組織構造を通じて能力を向上させることにより、この問題に対応しようとしている[26]。ネットワークシステム及び情報システムのセキュリティに関する指令[27]は、欧州連合全域にわたるネットワークシステム及び情報システムの安全性のミニマムのレベルを定めた。その指令の全ての構成国による全面実装は、サイバー回復力を拡大するために重要である:それは、鍵となる最初のステップである。一般データ保護規則は、職務権限を有する機関に対して個人データの侵害を通知すべき義務を導入した。別の鍵となる措置は、より強力で現代化された欧州連合のサイバーセキュリティ局、及び、消費者の信頼を構築するための ICT 製品と ICT サービスのための EU の認証枠組みである[28]。サイバーセキュリティソリューションの開発及び配備のための構成国の能力センターのネットワークを補助し、並びに、EU レベル及び国内レベルのこの領域における能力構築の努力の補完する作業も進行中である。この作業は、6 月 6 日に欧州委員会から提示され、サイバーセキュリティへの EU の投資の新たな優先順位を提供するデジタル欧州計画[29]の作業を描くことになる。

それと同時に、大規模なサイバーセキュリティインシデント及び危機への協調対応に関する勧告

[26] 欧州の領域における技術革新の強化の枠組み内において、サイバーセキュリティにおける作業をスケールアップするための EU の領域全体の新たな領域間パイロット活動が、2017 年 12 月に開始された。

[27] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[28] COM (2017) 477.

[29] Proposal for a Regulation establishing the Digital Europe programme for the period 2021-2027, COM(2018) 434.

（「青写真」）[30]は、国境を越える大規模サイバー攻撃に対応する際、構成国及び様々な EU の関係機関の間でどのような調整の仕事が行われるべきかを定めた。その勧告は、技術レベル、運用レベル及び戦略／政策レベルにおける実効的な調整のための状況認識の重要な役割を強調している。ネットワークシステム及び情報システムのセキュリティに関する指令に基づいて設置された協力グループもまた、関係者間の情報の交換及び共有を拡大するための作業をし、インシデントを表現するための共通の分類を策定している。このアプローチは、来るべき演習において試されることになる。現在の生起しつるあるサイバー脅威の戦略的分析は、構成国の諜報機関の貢献に基づき、Hybrid Fusion Cell から提供される。

不正なサイバー活動への EU の外交上の共同対応に関する枠組み（「サイバー外交ツールボックス」）は、EU の政治上の利益、安全保障上の利益及び経済的利益を損なう活動への EU の対応を強化するために使用され得る禁止措置を含め、共通の外国及び安全保障政策に基づく措置を定めるものであり、運用面における大きな前進であった。構成国によってこれが全面的に利用されればされるほど、それは、実効的な抑止策として機能する。この 4 月、外務理事会は、不正なサイバー活動に関する決議を採択した。それは、EU 及びそれ以外の国々において大きな損害と経済的損失を生じさせた Wannacry 攻撃及び NotPetya 攻撃を含め、情報通信技術の不正な利用を強く非難するものであった。

EU 及びその構成国は、少なくとも、情報の共有を介して、サイバー攻撃の属性を判断する構成国の能力を向上させる必要性がある。属性判断は、潜在的な侵略者を検知し得るものであり、そして、それらの職責が適正に説明責任を負うものとなる可能性を増加させ得るものである。検知を増加させることは、サイバーセキュリティを拡大することに向けた欧州委員会の戦略的なアプローチの重要な目標の 1 つである。刑事手続のための電子証拠の国境を越える収集の向上を狙いとする近時の欧州委員会提案もまた、サイバー犯罪を捜査し、訴追するための法執行機関の能力を大きく拡大することになるであろう。

強力なサイバー回復力は、集団的かつ広範囲のアプローチを必要とする。このことは、構成国における、並びに、EU 自身の機関、部局、外交、任務及び業務遂行におけるサイバーセキュリティを向上させ、かつ、サイバー攻撃に対応するためのより堅牢で実効的な構造を要求する：すなわち、欧州の機関の間における共通の安全な通信ネットワークが欠けていることは、重視すべき欠点である。EU の機関及びその職員におけるサイバーセキュリティの認識は、セキュリティの文化の向上と訓練強化によって増強されなければならない。

将来のステップ

- 欧州議会及び理事会は、本年末までに、合意により、サイバーセキュリティ提案の交渉を完了させるための作業を加速させなければならず、かつ、電子証拠収集に関する立法提案に迅速に合意しなければならない。
- 欧州委員会及び上級代表は、欧州全域の危機管理メカニズム及び危機対応メカニズムのサイバーな側面を高度化させるため、構成国と緊密に連携して、作業を行う。構成国は、サイバー攻撃の属性判断に関し、及び、サイバー攻撃に対する政治的な対応を強化するためのサイバー外交ツールボックスの実践的な使用に関し、構成国の作業を継続することが求められる。
- 我々のサイバー防衛能力を強化すべき必要に応えて、専門的な訓練及び教育プラットフォー

[30] C(2017) 6100.

ムは、構成国から提示された共同サイバー防衛訓練の機会を支援するために強化され続けている。同様の北大西洋条約機構の努力との間の波及効果も求められることになる。

3.5. 敵対的な諜報活動に対する回復力の構築

敵対的な諜報活動に対抗することは、何よりもまず、関連する EU の法令及び国内法並びに協定に従い、構成国間における拡大され、実効的な調整を必要とする。しかしながら、特に EU の機関に直接に向けられた活動のような脅威の増大に対抗するための EU の機関の能力を増加させること、そして、訓練及び物理的な防護の改善によって支援されたセキュリティの文化の意識を構築することも喫緊の課題である。EU の機関は、より堅牢な EU の認定制度を構築するためにも、構成国と作業を行い得る。そのような制度は、可能的な敵対者について、就中、構成国によって既に識別されている敵対者について、構成国及び EU の機関の間における認識の向上を可能とする積極的な通報を基盤とするものとし得る。

構成国間における、並びに、構成国と他の関連国際組織との間、とりわけ、北大西洋条約機構との間の共働関係は、EU 内における敵対活動に対する防諜活動の梃入れを支援し得るものである。構成国間の共働の増加からの利益を享受し得る分野の例の 1 つは、安全保障または公共の秩序を根拠とする構成国による外国からの直接の投資のスクリーニングに関し、欧州委員会から 2017 年 9 月に提案された規則案[31]に基づく投資のスクリーニングである。敵対的な諜報機関は、手の込んだ金融スキームを介して、EU に敵対的な彼らの活動の手段への資金供給を増加させているので、構成国間の共同活動を増加させることは、金融取引の精査のためにも同様に重要なものであり得る。

将来のステップ

- 欧州対外行動局及び欧州委員会は、特に EU の機関に直接に向けられた敵対的な諜報活動に対抗するために構成国と連携するための EU の能力を維持し、発展させるための改善された実践的な措置を設ける。
- 拡大された Hybrid Fusion Cell は、個人または機関に向けられたものであるおそれのある敵対的な諜報活動の性質の詳細分析及び報告を提供するため、防諜の専門知識によって補われる。
- 欧州議会及び理事会は、本年末までに、投資スクリーニング提案に関する交渉を完了するための作業を加速する。

4. 結 論

ハイブリッドな脅威、並びに、化学兵器、生物兵器、放射線兵器及び核兵器と関連する脅威は、EU のレーダー画面上では高程度のものであった。英国における 3 月のインシデントは、ハイブリッド戦争の広範なスペクトラム、並びに、化学兵器、生物兵器、放射線兵器及び核兵器と関連する脅威に直面する際の回復力の特段の必要性を際立たせるものであった。

[31] Proposal for a Regulation of the European Parliament and of the Council establishing a framework for screening of foreign direct investments into the European Union, COM(2017) 487.

欧州委員会及び上級代表は、ハイブリッドな脅威によって示された検討課題に対処するための多数の取り組みを採択し、かつ、提案した。欧州委員会は、化学兵器、生物兵器、放射線兵器及び核兵器のセキュリティリスクに対する準備体制を拡大するための 2017 年の行動計画の実装も加速させているところである。

この共同通知は、欧州理事会に対して既に遂行中の作業の情報を提供するためのものであり、そして、これらの脅威への対処のための EU の基本的な貢献を更に深化させ、強化するための行動が予定されなければならない分野を識別するためのものである。迅速なフォローアップを確保すべきなのは、まさに構成国、欧州委員会及び上級代表である。