ハイブリッドな脅威報告書（JOIN (2017) 30）
[参考訳]

2017 年 8 月 12 日
明治大学法学部教授
夏 井 高 人

＊＊＊

JOINT REPORT TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of the Joint Framework on countering hybrid threats - a European Union response（JOIN/2017/030 final）のテキスト（英語版）に基づき、和訳を試みた。テキストは、下記の Eur-lex の Web サイトから入手した。

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0030&from=EN
[2017 年 8 月 4 日確認]

報告書 JOIN/2017/030 final（以下「ハイブリッドな脅威報告書」という。）の作成日付・場所は、2017 年 7 月 19 日・ブリュッセルである。

この参考訳では、ハイブリッドな脅威報告書の全文を訳出した。

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。

ただし、意訳の語彙上の選択基準は、個々の法令の制定趣旨や当該法令の起草者の個人的趣味や歴史的変遷等を反映せざるを得ない部分があるので、個々の法令により一定せず、常に個別的なケースバイケースの検討が求められる。それゆえ、一般の英語教育上の慣例や翻訳家の慣例とは異なる訳となっている部分がある。

この参考訳は、あくまでもハイブリッドな脅威報告書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。

一般に、サイバー犯罪は、平時の法である刑事法のレベルでは個々の犯罪の一種として個別に考察されるのが普通である。しかし、例えば、「state sponsored attack」のような場合、国家の全てのインフラ、産業及び社会生活の全ての破壊を目的として実行されることがあり得るのであり、とりわけ、現在の IoT 環境においては、そのようなトータル攻撃を極めて容易に実行することが可能である。この場合、国家の存立が本来の保護法益であると理解すべきであり、そのための手段である個々のサイバー犯罪行為は手段的な行為として牽連犯のような状態になっていると理解するのが正しい。しかし、現時点の日本国の刑法学の主流においては、このような考え方を是認する傾向は、ほぼ皆無である。

トータル攻撃としてのサイバー攻撃は、核攻撃よりも深刻な結果を発生させ得る。そのことをどの程度まで考慮に入れ、そして、刑法解釈学上の考察の中に組み入れるかは、各人の学問の自由及び思想・信条の自由の領域に属する。

この報告書の中で引用されているユンケル委員長の「State of the Union 2016」は、下記のサイトで公表されている。

https://ec.europa.eu/commission/state-union-2016_en
[2017 年 8 月 4 日確認]

「a Europe that protects」は、「a Europe that protects, empowers and defends」の重要な一部である。これについては、欧州委員会の下記のプレスリリースがある。その中では、副委員長 Frans Timmermans 氏の発言が「First Vice-President Frans Timmermans said: "In this challenging era, we must work harder together and help to protect, empower and defend Europe's citizens」として引用されている。すなわち、保護の対象は、EU の市民である。

Juncker Commission presents third annual Work Programme: Delivering a Europe that protects, empowers and defends
http://europa.eu/rapid/press-release_IP-16-3500_en.htm
[2017 年 8 月 4 日確認]

この報告書の手段である「Hybrid threat」は、日本国においては、まだ馴染みの薄い概念かもしれない。

しかし、例えば、フランスの大統領選挙等に見られたように、現実の選挙活動を妨害し、攻撃国にとって不利となる可能性のある指導者が権力を握ることを阻止するために、古典的な

扇動行為と電子的なサイバー攻撃とが効果的に組み合わされて用いられる場合がその典型例であると考えることができる。また、例えば、ウクライナの例のような、電力網に対する大規模なサイバー攻撃により、攻撃を受けた国のインフラを麻痺させ、生産力や防衛力を根こそぎ無力化してしまうような攻撃を想定することもできる。そのような攻撃では、リアルな世界に対する物理攻撃とサイバー空間に対する電子的な攻撃とが完全に一体のものとして存在しており、それぞれが全体的な戦略の中における戦術の一部となっている。

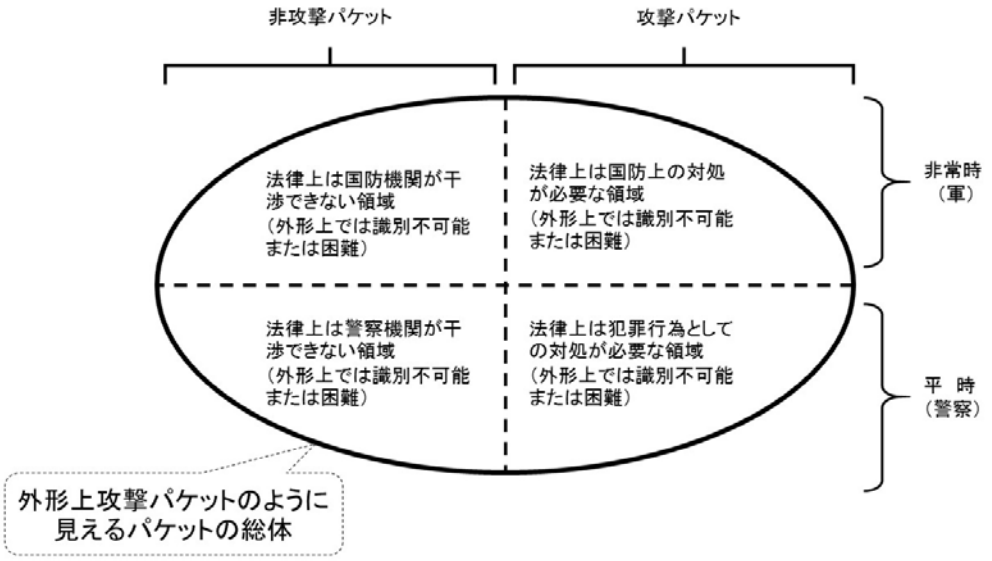
そのようなトータル攻撃が可能となるのは、サイバー空間における電子的な仕組みの多くが現実世界における社会の機能を統御するための手段として存在しているからである（例：電子政府）。しかも、IoT またはモノのインターネット（Internet of Things）の大規模かつ広範な普及、あるいは、SNS に代表されるような便利なコミュニケーションツールの普及と日常化は、そのような攻撃の成功率を著しく高めるものであるということができる。人心攪乱という策略（戦術）は、非常に古い時代から存在し、例えば、中国においても、『史記』、『荀子』、『韓非子』または『孫子』の中でその本質が述べられている。しかし、現代社会においては、電子的な方法を用い、ごく少数の人間によって、攻撃対象である社会全体に対しほぼ網羅的かつ効率的に悪影響を与えることができるという点が基本的に異なっている。従来からあるようなマルウェアの使用や標的型攻撃の実行だけではなく、特殊なチャットボットの類の濫用によって、エージェントによる自動的な攻撃が可能となっていることも無視できない。現代社会における IoT やクラウドという社会基盤が上記のような意味での社会の最大の脆弱性要素となっていることを正確に評価・理解し、欠陥を欠陥として冷静に承認した上で、合理的な防護策を検討することが重要である。

更に、個別的なサイバー犯罪のための攻撃パケットと軍事目的によるサイバー戦のための攻撃パケットとを外見から識別することはできない（下図参照）。とりわけ、主観的な目的ないし意図が異なるだけで、同一のマルウェアや攻撃手法を用いている場合には、攻撃パケットとしては全く同一である。しかも、それらが日常的に混在して存在している。それゆえ、現代社会は、戦時と平時が常に共存する状況に下にある。

加えて、超小型のドローン、サイボーグ化された小動物等を GPS の機能を用いて自動的に攻撃対象地まで到達させ、生物化学兵器を散布するような攻撃もサイバーとリアルを組み合わせた攻撃の一種である。合成された人工生命体（ミュータント）によっても同じ結果が得られる。このようなタイプの攻撃者に対しては、国家または組織の倫理委員会による統制は一切及ばない。そして、このようなタイプの攻撃に対する防御方法は、ほぼ存在しないと言うことができる。この報告書の中において、「行動 10（Action 10）」と関連して、保健当局や食品当局に関する言及があるのは、そのためである。しかし、これらの当局による防御が可能なのは、人間による制御・対応が可能な生物化学兵器に対してのみである。とりわけ、自己増

殖可能で有毒な有機体ロボットまたは有毒ミュータントの場合、識別された個体を破壊したとしても、それだけでは脅威を完全に消滅させたことにならない。また、理論的には、その分子構造上または生体構造上、それに対応するワクチンの製造があり得ないようなものも存在し得る。その意味で、全人類は、絶滅寸前の段階にあると言い得る。

「Hybrid threat」は、このようなものとして理解されるべきである。



総括的な感想として、この報告書は、「情報法（Information Law）とは何か？」及び「情報法の主たる対象領域は何であるのか？」を考える上でも極めて重要な示唆を提供する公式文書の 1 つであると考える。

一般に、「情報法」という学問領域は、デジタル著作権のような知的財産権の情報的な側面のみを対象とする学問ではないし、個人データ保護関連の法令のみを取り扱うものでもなく、情報に対するアクセス権のみを主眼とするものでもない。これらの部分的な分野のみを取り扱う書籍でありながら『情報法』を標題とするものが散見されるけれども、そのような書籍は、情報法の本体部分を取り扱う書籍ではない。

「情報法」を名乗ることのできる書籍は、少なくとも、情報技術、情報通信、情報ネットワーク及び情報インフラを法的に基礎づける公法上の根拠法令、これらの技術を基盤とする情報及び情報財のやりとり及び国家機能の遂行を規律する公法上及び私法上の様々な法令、そして、そのような情報基盤それ自体及び情報基盤上で生起する様々な法律行為や事実行為に伴う法的紛争の解決のための公法上及び私法上の法令、刑罰法令及び司法制度と国際共助を含むものでなければならず、加えて、これらの総体としての情報社会を守るための法令や国際的な規範、並びに、グローバルな情報社会の秩序維持の根拠となる準拠法、

国際法及び情報セキュリティと関連する国際標準等を含めるものでなければならない。

（この参考訳を作成する際に考慮した事項）

「resilience」の概念は、分野によって異なる意味で用いられるのが普通であり、一般に、「復元力」、「回復力」、「抵抗力」、「耐久力」等と訳されている。EU のサイバーセキュリティ関連法制の中では、攻撃を事前に探知するという文脈よりもむしろ、現に攻撃が実行されている最中またはその後におけるインフラの可及的速やかな能力回復を主眼としてこの語が用いられる場合が多い。しかも、その語義または用法は、過去数年間において微妙に変化しつつあるようにも思われる。

特に、国家政策としての「resilience」は、情報システムの防御のための具体的な手法というよりは、より広い戦略目標の一種である。それは、国家安全保障政策ないし軍事政策全体を包含し得るものである。それゆえ、「resilience」を情報セキュリティの分野における技術的手段の一種として矮小化してとらえることは、非常に危険である。

この参考訳においては、とりあえず、文脈に応じて、「resilience」を「回復力」または「回復性」と訳すことにした。

「solidarity」は、一般に、「連帯」または「団結」と訳されている。

しかし、TFEU の第 222 条第 1 項（solidarity 条項）は、「solidarity」の実質的意味内容として、EU または構成国の民主主義国家体制を破壊し得る大規模なテロ攻撃または大規模な武力衝突または軍事衝突が発生した場合に、EU の構成国及びその軍が連携して、そのような攻撃または紛争に対処し、武力をもって撃退・解決するための統括的な軍事行動を実施することを示している。これは、そのような構成国が連携して実施される軍事行動のための EU の一次法としての法的根拠を提供するものである。要するに、「統括的軍事防衛行動」を意味するのであって、EU の市民のレベルにおける平時の相互協力や相互扶助のようなもの、あるいは、市民運動や労働運動における団結のようなものを指すものではない。あくまでも、EU 構成国の集団的防衛権の行使の場面における構成国間の「solidarity」のことを意味する。

それゆえ、この参考訳では、TFEU の第 222 条第 1 項における「solidarity」を、「連帯」ではなく、「連携」と訳すことにした。

「risk assessment」は、そのまま、「リスク評価」と訳すことにした。しかし、その目的、実質的な内容、評価手法・手段等が、例えば、個人データの処理におけるリスク評価（プライバシー影響評価）と同じ性質・機能をもつものであるか否かについては疑問が残る。このことは、環

境影響評価においても同じである。それゆえ、「risk assessment」の訳語は訳語として、それにこだわることなく、「risk assessment」の実質的な内容や機能について、更に綿密に実証的かつ帰納的な研究が深められなければならない。これは、今後の研究課題の 1 つである。

（訳出済みの関連法令等及び参考文献）

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。指令 2013/40/EU の参考訳・改訂版は、法と情報雑誌 2 巻 8 号 164～184 頁にある。サイバー犯罪条約（ETS No.185）の説明書の参考訳は、法と情報雑誌 1 巻 6 号 1～132 頁にある。指令(EU) 2017/541 の参考訳は、法と情報雑誌 2 巻 8 号 1～29 頁にある。 PNR 指令(EU)2016/681 の参考訳は、法と情報雑誌 2 巻 3 号 119～155 頁にある。API 指令 2004/82/EC の参考訳は、法と情報雑誌 2 巻 5 号 60～70 頁にある。Europol 規則 (EU)2016/794 の参考訳は、法と情報雑誌 2 巻 3 号 1～101 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した文献等のほか、藤井秀之「サイバー空間におけるレジリエンスによる抑止」InfoCom Review 69 号 75～87 頁(2017) を参考にした。

＊＊＊

ハイブリッドな脅威への対抗に関する共同枠組みの実装に関する欧州委員会から欧州議会及び理事会宛の共同報告書－欧州連合の対応－ JOIN (2017) 30 final

1. イントロダクション

EU は、その中で最大の安全保障上の課題と直面している。脅威は、次第に、在来型のものとは異なる形態をとるようになってきており、ある場合には、新たなテロリズムの形態のような物理的なものであり、ある場合には、複雑なサイバー攻撃をデジタル空間で用いるものである。他の場合には、偽情報キャンペーンやメディア操作を含め、より巧妙なものであり、そして、圧力の強制的な応用を狙いとするものである。それらは、人間の尊厳、自由及び民主主義のような欧州の核となる価値観を掘り崩そうとしている。近時の地球規模の連携したサイバー攻撃は、その属性が挑戦的なものであったことが証明され、我々の社会と組織の脆弱性を明らかにするものであった。

2016 年 4 月、欧州委員会及び上級代表は、ハイブリッドな脅威への対抗に関する共同通知（共同枠組み）[1]を採択した。ハイブリッドな脅威の国境を越える複雑な性質を認識して、この枠組みは、我々の社会の包括的な回復力を強化に向けた全政府のアプローチを提示する。理事会 [2]は、この取り組み及び行動の提案に賛成し、欧州委員会及び上級代表に対し、2017 年 7 月までに進捗状況に関して報告するように勧奨した。EU は、ハイブリッドな脅威に対する構成国の回復力の構築のために構成国を支援することができるが、国内の安全保障及び防衛と関連するハイブリッドな脅威に対する対応である限り、その第一次的な責任は、構成国にある。

ハイブリッドな脅威への対抗のためのこの共同枠組みは、EU の安全保障及び防衛のための包括的かつより統合された取り組みの重要な一部を構成する。2016 年 9 月の講演「欧州連合の状態」の中でユンケル委員長から求められたように、この枠組みは、保護する欧州の創設に貢献する。2016 年、欧州連合も、より大きな保護を求める市民の期待に応えるためのより強固な欧州防衛政策のための基礎を築いた。EU の外交及び安全保障政策のための EU グローバル戦略[3]は、域内の回復力と EU の対外活動とを連携させる統合的な取り組みの必要性を詳しく述べ、また、防錆政策と、域内市場、産業、法執行及び諜報機関を包摂する政策との相乗効果を求めた。2016 年 11 月における欧州防衛行動計画の採択の後、欧州委員会は、防衛サプライチェーンにおける回復力の育成及び防衛のための単一市場の強化によってハイブリッドな脅威に対応する

[1] Joint Communication to the European Parliament and the Council Joint Framework on countering hybrid threats – a European Union response, JOIN (2016) 18 final.
[2] Council conclusions on countering hybrid threats, Press Release 196/16, 19 April 2016.
[3] 2016 年 6 月 28 日の High Representative to the European Council によって示された。

ための EU の能力に貢献する具体的な取り組みを提案した。とりわけ、2017 年 6 月 7 日、欧州委員会は、2020 年までに 6 億ユーロの、そして、2020 年以降は年間 1 億 5000 万ユーロの基金案による欧州防衛基金を開始した。欧州の安全性通知 [1]は、ハイブリッドな脅威に対抗する必要性及び安全保障の分野における域内活動と対外活動との間のより大きな一貫性を確保することの重要性を認識した。

EU の指導者達は、欧州の将来に関する討論の中の中央ステージに安全保障及び防衛を位置付けた [2]。これは、欧州連合の共有の安全保障及び防衛の強化に向けた安全で防護された欧州連合のビジョンを定める 2017 年 3 月 25 日のローマ宣言の中で承認された。欧州理事会議長、欧州委員会及び北大西洋条約機構事務総長は、EU と NATO の戦略パートナーシップに新たな推進力と新たな実質を与えるために、2016 年 6 月 8 日、ワルシャワにおいて、共同宣言書に署名した。

この共同宣言は、ハイブリッドな脅威への対抗を含め、2 つの組織の間の協力が拡大されるべき 7 つの具体的な分野を示した。実装のための 42 の提案の共通のセットは、その後、EU 及び NATO 理事会の両者によって承認され、そして、その実質的な進捗を示す報告書が 2017 年 6 月に発行された [3]。

2017 年 6 月に提示された欧州の防衛の将来に関する欧州委員会のリフレクションペーパー[4]は、欧州が直面している増大する安全保障上及び防衛上の脅威に対していかに対応するか、及び、欧州自体の防衛能力を 2025 年までにいかに拡大するかに関し、異なるシナリオを示している。合計 3 つのシナリオの中で、安全保障及び防衛は、自国及び外国における我々の利益を保護し、向上させるため、欧州のプロジェクトの統合された要素の一部として考えられている。欧州は、安全保障の提供者とならなければならず、かつ、欧州自身の安全保障を徐々に確保しなければならない。単一の構成国だけがこの課題、とりわけ、ハイブリッドな脅威への対抗という課題と直面するということはあり得ない。それゆえ、防衛及び安全保障上の協力は、選択的なものではない：保護する欧州の上で実現する必要がある。

この報告書の目的は、共同枠組みの中で提案された 4 つの分野、すなわち、状況認識の向上；回復力の構築、危機を回避し、対処するため、及び、連携した復旧のための構成国及び欧州連合の能力の強化；並びに、手段の相補性を確保するための NATO との協力拡大の各分野における行動に関する進捗状況及び次の実装段階についての考察を提供することにある。この報告

[1] COM (2016) 230 final, 20.4.2016.
[2] 2016 年 9 月 16 日の欧州理事会のブラチスラヴァ・ロードマップ及び 2017 年 3 月 25 日の 27 構成国、欧州理事会、欧州議会及び欧州委員会のローマ宣言
[3] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation
[4] Reflection paper on the future of European defence, 7.6.2017
https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf

書は、効果的で真に安全な欧州連合に向けた月次進捗報告書と併せて読まれるべきである。

2. 脅威のハイブリッドな性質の認識

ハイブリッドな活動は、欧州の安全保障環境で頻発する特徴となってきている。これらの活動の強度は、偽情報キャンペーン、悪意あるサイバー活動及び社会の脆弱な構成員を彼らの代理行為者として過激化させようとするハイブリッド行為の加害者による選挙妨害の懸念が増すにつれて増大している。ハイブリッドな脅威に対する脆弱性は、国境内だけに限定されるものではない。ハイブリッドな脅威は、EU 及び NATO のレベルの連携した対応も必要とする。2016 年 4 月以降の発展は、脅威が、今なお、しばしば、孤立して評価されているとはいえ、観察された活動の幾つかのハイブリッドな性質及び協力活動の必要性について、欧州連合内の認識と理解が向上してきているということを示している。EU は、状況認識及び協力を向上させるためのその取り組みを継続することであろう。

行動 1:構成国は、欧州委員会及び上級代表の適切な支援を受け、特別のハイブリッド関連性指標を含め、国内及び欧州全体の構造とネットワークに悪影響を及ぼし得る主要な脆弱性を特定するためのハイブリッドリスク調査を開始することを勧奨される。

理事会は、そのグループがハイブリッドな脅威の鍵となる指標をより良く特定できるようにする一般的な調査を構築し、それを早期警戒及び既存のリスク評価メカニズムの中に組み入れ、そして、それを適切に共有するために、構成国から専門家を結集し、「議長の友」グループを設けた。付託条項が合意され、作業は既に開始された。一般的な調査は、その準備の後に実際の調査が開始される 2017 年末までに準備を終えるものとしなければならない。ハイブリッドな脅威に対する防護は、相互に強化されなければならない。それゆえ、構成国は、脆弱性の範囲及び全欧における準備状況に関する重要な情報を提供するため、可能な限り速やかに、この調査を実施することが推奨される。

A 認識の向上

情報解析及び評価作業を共有することは、不確実性を減少させ、そして、状況認識を拡大するための重要なツールの 1 つである。過去 1 年間に著しい進歩が見られた。EU Hybrid Fusion Cell が設置され、現在、完全に稼働している。East Stratcom Task Force が置かれ、フィンランドは、ハイブリッド脅威に対抗するための欧州センターを開始した。EU Stratcom Task Force East、Hybrid

Fusion Cell 及び NATO との間にある良い協力関係の下で、偽情報またはプロパガンダにおけるツールとレバーを解析することに多くの作業が焦点を当ててきた。これは、ハイブリッドなレンズを介して、我々の域内安全保障及び域外安全保障に対する脅威の解析及び評価のより深く刻まれた文化の構築を継続するための良い基礎を形成している。

EU Hybrid Fusion Cell

行動 2:ハイブリッドな脅威に関する機密情報及びオープンソースの情報の受信及び解析をすることができる EU Hybrid Fusion Cell を既存の EU 諜報及び情報センター（EU Intelligence and Situation Center）の組織内に創設すること。構成国は、EU Hybrid Fusion Cell との協力及び安全な通信を確保するため、ハイブリッドな脅威に関する国内連絡部局を設置することが勧奨される。

ハイブリッドな脅威に関する異なる関係者からの機密情報及びオープンソースの情報を受信し、解析するために、EU 諜報及び情報センターの組織内に EU Hybrid Fusion Cell が設置された。そして、解析は、EU 及び大半の構成国の中で共有され、そして、それらは、EU レベルで行われる安全保障リスク評価への入力を含め、EU の意思決定プロセスに情報伝達する。EU 軍参謀情報本部は、軍の解析によって Fusion Cell の作業に寄与する。今日までに、ハイブリッドトピックスに関する 50 の評価及びブリーフィングが作成された。2017 年 1 月以来、現在の脅威とハイブリッド問題を解析する『Hybrid Bulletin』を定期的に作成し、EU の機関及び組織並びに国内連絡部局内でそれを直接に共有した [1]。Cell の全業務遂行能力は、予定どおりに、2017 年 3 月までに達成された。最後に、Fusion Cell の創設の際に得られた教訓の共有と（機密情報の交換に関する EU の法令を完全に遵守して行われる）情報の共有の両方に関し、NATO の新生ハイブリッド解析部門との職員間の関わりが進行中である。EU Hybrid Fusion Cell は、現在、更に協力を拡大するための別の取り組みを検討中であり、そして、2017 年秋に計画されている EU-NATO パラレル演習において重要な役割を演ずることであろう。その演習では、EU Hybrid Fusion Cell の対応力がテストされ、そして、確認された訓練が組み込まれることになる。

戦略的な通信

行動 3:上級代表は、積極的な戦略的通信を提供し、メディア監視及び言語専門家の利用を最

[1] 今日までに、21 の構成国が国内連絡部局を任命した。構成国の首都において、政策上の役割／回復力の役割において仕事をする個人が存在する。

適化するための能力を最新のものに改め統括するための方法を構成国と検討する。

最近数か月、攻撃相手を弱体化させるために使用される手段のスペクトラムの中で、ソーシャルメディア内の偽情報キャンペーン及び組織的な偽ニューズの配信が増加している。ソーシャルメディアが優先的なプラットフォームである場合、信頼性があり正当であるように見える情報は、誰か個人、組織または政府にとって利益に、公衆の意見を変更し得る。これらのハイブリッドな戦術は、我々の社会に混乱を発生させ、民主的な政府及び我々の体制、機関及び選挙に不信をもたせるというより広い目標をもっている。偽ニューズは、しばしば、オンラインのプラットフォームを介して拡散される（行動 17 参照）。欧州委員会及び上級代表は、誤報と闘うためにオンラインプラットフォーム及びニューズメディアによって講じられた最近の措置に賛成する。欧州委員会は、そのような任意の措置を引き続き奨励する。

上級代表は、偽情報事案及び偽情報キャンペーンを予測し、これに対処する East Stratcom Task Force を設置した。これは、それらの国々におけるメディア環境も強化しつつ、東欧諸国における欧州連合の政策に関する意見交換を大きく改善している。Task Force は、2 年以上にわたり、18 の言語による 3000 以上の個別の偽情報案件を明らかにしてきた。開始予定となっているオンライン検索機能をもつ新たな Web サイト「#EUvsdisinformation」は、利用者のアクセスを大幅に改善することであろう。しかしながら、調査分析作業の結果は、偽情報の経路の数及び 1 日あたりの拡散されるメッセージの数は、大幅に増えてきている。Horizon 2020 によって資金付けられている EU-STRAT プロジェクトは、東パートナーシップ諸国における政策及びメディアを解析する。

上級代表は、ハイブリッドな脅威の増加に対し、より効果的に対抗するために、StratCom Task Forces の作業を支援するよう構成国に勧奨している。このことは、Task Force South が、アラビア語のものを含め、欧州連合及びその政策に関する事実の神話を破壊し、これを確実なものとするアラブ世界向けの通信及び配信を改善する助けとなるであろう。地域ジャーナリストとの交流は、ニューズ製品が文化的に調和のとれたものであることを確保することの助けとなるであろう。これら 2 つの Task Force は、EU Hybrid Fusion Cell の支援を受け、構成国の関連する取り組みを支援し補完することを狙いとしている。加えて、欧州委員会は、偽情報に関するものを含め、暴力的な過激主義に対抗する戦略的な通信の使用に関する解析、グッドプラクティス及びアイデアを共有する 26 の構成国の共同的ネットワークである欧州戦略通信ネットワークに共同で資金提供している。

「ハイブリッドな脅威への対抗」の研究拠点

行動 4：構成国は、「ハイブリッドな脅威への対抗」の研究拠点を設けることを検討するように勧奨

される。

拠点を設けることの求めに応じて、2017 年 4 月、フィンランドは、ハイブリッド脅威への対抗の欧州研究拠点を開始した。EU の構成国 [1]、ノルウェー及び合衆国がその構成員であり、欧州連合及び NATO は、共に、運営委員会を支援するために招請された [2]。拠点の任務は、ハイブリッドな脅威への対抗を支援するために、戦略的な対話を奨励すること、並びに、回復力及び対応能力の改善に意欲のあるコミュニティと共に調査及び解析の作業を行うことである。拠点は、将来のハイブリッド演習のための場を提供することも期待されている。拠点は、既に、EU Hybrid Fusion Cell との密接な連絡を確立し、2 つの組織の仕事が相互に補完されることになる。EU は、現在、EU が拠点に対して提供することのできる具体的な支援について検討中である。

B. 回復力の構築

共同枠組みは、（例えば、輸送、通信、エネルギー、金融または地域社会インフラの）回復性を、プロパガンダや情報キャンペーン、企業活動、社会及び経済の流れを弱体化させる試み、並びに、情報技術及びサイバー関連インフラに対する攻撃に対抗するための EU の活動の中心部分に置いている。共同枠組みは、回復性を、社会を結束させ、EU の内外における危機の拡大を回避するための予防的かつ抑制的な行動として理解している。EU の付加価値は、既存の法律文書及び計画に広範に依拠して、それらの回復力を構築するために、構成国及びパートナーを支援することにある。サイバーセキュリティ、重要インフラ、不正使用に対する金融システムの保護及び暴力的な過激主義及び過激化に対抗するための取り組みのような分野において、回復力を構築するための活動の中で、大きな進展があった。

重要インフラの保護

行動 5:欧州委員会は、構成国及び利害関係者と協力して、関連分野におけるハイブリッドな脅威に対する重要インフラの保護及び回復性を向上させるために、指標を含め、共通のツールを指定する。

欧州重要インフラ保護計画（EPCIP）の遂行過程において、欧州委員会は、関連分野における

[1] フィンランド、フランス、ドイツ、ラトビア、リトアニア、ポーランド、スウェーデン、英国、エストニア、スペイン

[2] センターは、他の EU 構成国及び NATO 加盟国が参加するために開かれている。

ハイブリッドな脅威に対する重要インフラの保護及び回復性を向上させるために、脆弱性指標を含め、共通のツールを指定するための作業を進めた。2017 年 5 月、欧州委員会は、重要インフラに対するハイブリッドな脅威に関するワークショップを開催した。その参加者の中には、ほぼ全ての構成国、EU Hybrid Fusion Cell 及びオブザーバーとしての NATO が含まれていた。構成国内の国内機関に対するアンケート調査に基づき、将来の活動のための共通のロードマップ及びステップが承認された。欧州委員会は、2017 年末までに指標に関する合意を得ることを目指し、この秋に、利害関係者と更に協議する。

欧州防衛機関は、共通の能力を指定し、エネルギーインフラの連鎖から生ずる欠点及び防衛能力を調査するために作業をしている。欧州防衛機関は、2017 年秋に概念規定書及び全体的方法論のためのパイロット行動計画書を作成する。

EU のエネルギー供給安全保障の強化

行動 6:欧州委員会は、構成国と協力して、エネルギー源の多様化のための取り組みを支援し、原子力インフラの回復力を強化するための安全性及び防護基準を促進する。

欧州委員会は、2016 年 12 月及び 2017 年 4 月、供給の防護パッケージの中で具体的な提案を行い、理事会及び欧州議会は、ガス供給危機を回避することを狙いとする新たなガス供給防護規則に関する合意に至った。新たな法令は、構成国の間の供給手段の安全性のための地域的な連携による共通の取り組みを確保するであろう。このことは、危機またはハイブリッド攻撃の場合において、ガス不足に対する準備をし、それを管理するために、EU をより良い立場に置くことになる。構成国は、重大な危機または攻撃が起きる際、欧州の家庭と企業がブラックアウトしてしまわないようにするために、近隣の構成国を支援することができるようになる。

EU は、エネルギー連合枠組み戦略及び欧州エネルギー防護戦略に沿って、EU のエネルギー供給の経路及び供給源を多様化する重要なプロジェクトの発展においても、大きく進展させた。例えば、南ガス回廊計画に関しては、全ての主要なパイプラインプロジェクト:すなわち、南コーカサスパイプライン、アナトリア横断パイプライン及びアドリア横断パイプライン、シャーデニス上流 II の拡張、及び、中央アジア特にトルクメニスタンへの南ガス回廊計画の拡張において、具体的な工事が進行中である。液化天然ガス（LNG）の欧州への輸入が増加しており、合衆国のように、新たなエネルギー源となりつつある。リトアニアの基地の事例は、多様化計画が単一の供給者への依存をいかに減少させものであるかを示している。エネルギー政策の強化及び固有のエネルギー源のより良い使用、とりわけ、再生可能エネルギーもまた、エネルギーの経路及びエネルギー源の多様化のために貢献している。

原子力の安全性の分野において、欧州委員会は、国内機関及び国内規制当局とのワークショップを介して、構成国が 2017 年末及び 2018 年末までにそれぞれ国内法化することが求められる 2 つの指令の一貫性のある効果的な実装を積極的に支援している。更に、欧州原子力共同体研究訓練計画は、原子力の安全性に寄与している。

輸送及び流通網の安全性

行動 7:欧州委員会は、輸送部門全体の新たな脅威を監視し、それが適切なときは、立法を新たなものに改める。EU 海上防護戦略及び EU 税関リスク評価戦略並びにそれらの行動計画の実装において、欧州委員会及び上級代表は、（それぞれの職務権限の範囲内で）構成国と連携して、ハイブリッドな脅威、とりわけ、輸送上の重要インフラに関するハイブリッドな脅威に対しいかに対応するかを検討する。

安全な欧州連合通知に沿って、欧州委員会は、EU レベルで、構成国、EU 諜報及び情報センター並びに関連機関と共に、輸送の安全性に関する脅威を特定し、効果的で比例的な解消策の開発を支援するための安全性リスク評価を促進している。2014 年のウクライナ東部上空におけるマレーシア航空 MH17 便の撃墜は、紛争地域の上空通過によって示されるリスクを際立たせた。紛争地域における欧州上級タスクフォースの勧告 [1]に沿って、欧州委員会は、民間航空会社及びセキュリティ専門家並びに EEAS の支援を得て、機密情報の交換及び共通リスク画像の定義をできるようにする「EU 共通リスク評価」のための手法を開発した。2017 年 3 月、欧州航空安全局（EASA）は、この EU 共通リスク評価の結果に基づき、最初の「Conflict Zones Information Bulletin」[2]を発行した。欧州委員会は、航空安全の分野において行われているリスク評価活動を他の輸送の場面（例：鉄道、海運）に拡大することを検討しており、2018 年にその提案が行われる。2017 年 6 月 1 日、欧州委員会、EEAS 及び構成国は、ギャップ及びリスクを解消するための可能な措置を検討するために、鉄道の安全性に関するリスク評価演習を開始した。

第 7 次枠組み計画及び Horizon 2020 の安全性調査プロジェクトにおいても、航空の安全及び航空管制（ATM）上の相当の努力が払われた。民間航空の分野において、欧州委員会は、欧州航空安全局及び利害関係者と共に、サイバーセキュリティを強化し、ハイブリッドな脅威と闘うための 2 つの新たな取り組みを発展させている：すなわち、航空に関するコンピュータ緊急対応チームの設置、そして、単一欧州航空管制について職責を負う単一欧州航空管制研究機関

[1] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf
[2] https://ad.easa.europa.eu/czib-docs/page-1

（SESAR）の共同事業におけるサイバーセキュリティに関するタスクフォースの設置である。欧州防衛機関は、SESAR の共同事業に対し、「サイバーセキュリティに関する欧州戦略統括プラットフォーム」を介して、航空サイバーに関する軍事上の入力を提供している。それは、構成国及び産業界の要請により、EU レベルで、航空に関する全ての活動の連携を支援する。航空におけるサイバーセキュリティに関するロードマップに沿って、2016 年、欧州航空管制局は、既存の法令のギャップ解析、とりわけ、欧州航空サイバーセキュリティ拠点の定義及び設置に関する解析を行った：現在、後者は、運用開始となっており、また、航空及び EUROCONTROL の脅威解析を行う（採択された協力のためのロードマップ）EU コンピュータ緊急対応チーム（CERT-EU）と協力し（2017 年 2 月に署名された了解覚書）、その一方で、オープンソースの解析結果の配布のための Web サイトを開発した。2017 年秋までに、標準化計画及び安全な情報交換が採択される。

税関リスク評価

税関という観点から、欧州委員会は、事前貨物情報及び税関リスク評価制度の大きな改訂に焦点を当てている。これは、国際的な流通網並びに関連する重要インフラの安全性及び完全性に対する脅威（例：輸入によって示される港湾施設、空港または地上国境への直接の脅威）と関連するものを含め、全範囲の税関上のリスクを包摂するものである。改訂の目的は、EU における税関当局が、物品の移動に関し、貿易事業者から全ての必要な情報を入手することを確保すること；税関当局が、この情報を、構成国間でより効果的に共有することができることを確保すること；税関当局が、構成国と共通の特別のリスク法令を適用することを確保すること；並びに、税関当局が、他の機関、とりわけ、法執行機関及び治安当局との間でより緊密に協力することによって、より効果的に、リスクのある運送に狙いを定めることができるようにすることを確保することにある。

欧州委員会によるこの改訂の実装に要する IT 開発は、現在のところ、緒に就いたところであり、今月中に、中央レベルで関連する投資が開始される。

宇宙

行動 8：宇宙戦略及び欧州防衛行動計画の遂行過程の範囲内において、欧州委員会は、とりわけ、宇宙探査及び追跡の適用範囲をハイブリッドな脅威に拡大する可能性、欧州のレベルにおける時世代 GovSatCom のための準備、並びに、時間の同期に依存する重要インフラへの Galileo の導入によって、ハイブリッドな脅威に対する宇宙インフラの回復性を強化するための提案をする。

欧州委員会は、2018 年に政府衛星通信（GovSatCom）及び宇宙探査及び追跡に関する規則上の枠組みを準備する際、ハイブリッドな脅威に対する回復力という側面をその評価の中に統合する。宇宙戦略に沿って、Galileo 及び Copernicus の進化を準備する際、欧州委員会は、それらのサービスが重要インフラの脆弱性を解消する助けとなる可能性について評価する。評価報告書は、2017 年秋に用意されなければならず、次世代の Copernicus 及び Galileo に関する提案は、2018 年に用意されなければならない。欧州国防機関は、宇宙ベースの通信、軍の位置づけ、ナビゲーション及びタイミング並びに地球の監視の分野において、能力開発プロジェクトの共同作業に従事する。全てのプロジェクトは、現在の生起しつつあるハイブリッドな脅威に照らし、回復性の要求事項に焦点を当てるものとなる。

防衛上の能力

行動 9：上級代表は、構成国から適切に支援を受けて、欧州委員会と連絡をとり、特に、1 つの構成国または複数の構成国に対するハイブリッドな脅威に対抗するために、いかにして防衛能力を適合させ、かつ、EU の能力を開発するかに関するプロジェクトを提案する。

2016 年及び 2017 年、欧州防衛機関は、欧州委員会、EEAS 及び構成国の専門家と共に、ハイブリッドな脅威のシナリオに関する 3 つの机上演習を行った。それらの結果は、能力開発計画の見直しの中に反映されることになり、そして、ハイブリッドな脅威に対応するために必要な来るべき鍵となる能力開発は、EU の新たな能力開発の優先事項の中に統合されることであろう。要求事項カタログ 2005 の改訂に関する作業は、ハイブリッドな脅威の場面を考慮に入れるものとなる。2017 年 4 月、欧州防衛機関は、重要な港湾インフラに対して向けられたハイブリッド攻撃から派生する軍事的な意味に関する解析報告書を仕上げた。それは、2017 年 10 月の海上保安専門家のワークショップにおいて討論されることになる。超小型ドローンへの対抗の関連における軍の役割についての別の特別の解析が 2018 年に予定されている。更に、構成国によって特定されたハイブリッドな脅威に対する回復力を強化するための能力上の優先事項は、2019 年度の欧州防衛基金に基づく支援を受けることができるであろう。欧州委員会は、共同立法者に対して、迅速な採択を確保することを求め、また、構成国に対して、ハイブリッドな脅威に対する EU の回復力を強化するための能力開発プロジェクトの提案を送付するように求めている。

行動 10：欧州委員会は、構成国と協力して、既存の準備及び共同の仕組み、すなわち、保健衛生委員会の範囲内で、ハイブリッドな脅威に対する認識及び回復力を向上させる。

保健制度及び食品制度の範囲内における能力開発を含め、ハイブリッドな脅威に対する準備及び回復力の強化という観点から、欧州委員会は、訓練と模擬演習を通じて、そして、体験ガイドライン及び資金共同活動の交換の促進によって、構成国を支援する。これは、とりわけ、健康に対する重大な国境を越える脅威に関する EU の保健衛生枠組みに基づき、かつ、急速に公衆に広まり、国境を越える保健上のリスクを世界規模で防止し、これに対応することを目的とし、構成国を含め 196 の国々で拘束力のある立法の柱である世界保健規則を実装するための公衆衛生計画に基づき、行われる。保健部門において部門横断的な準備及び応答をテストするために、欧州委員会の機関は、2017 年秋、複雑で多面的なハイブリッド脅威に関する演習を実施する。欧州委員会及び構成国は、EU レベルにおけるアクチン供給を強化し、保健衛生を向上させるために、ワクチンの供給と需要の予測、革新的なワクチン製造過程の研究を含め、ワクチン接種に関する共同活動を準備している（2018 年～2020 年）。欧州委員会は、保健上の脅威のより精密な特定及び発生源の確定のための先進的な科学的調査技術に対応し、並びに、食品の安全性の迅速な管理を生じさせる出来事に対応するため、欧州食品安全機関及び欧州疾病予防管理センターとも共同活動をする。欧州委員会は、いかなる重大な出来事に対しても 48 時間以内に対応する連携した研究のための研究式提供者のネットワーク（Global Research Collaboration for Infectious Disease Preparedness）を設置した。

行動 11：欧州委員会は、構成国に対し、優先的な事項として、28 CSIRT 及び CERT-EU（EU コンピュータ緊急対応チーム）との間のネットワーク並びに戦略的な協力のための枠組みを設け、これを完全に利用することを奨励する。欧州委員会は、構成国と連携して、サイバー脅威に関する部門別の取り組み（例：航空、エネルギー、海上保安）が、NIS 指令によって包摂される情報、専門性及び緊急対応を保持する部門横断的な能力と一貫性のあるものであることを確保しなければならない。

何千ものコンピュータシステムを使用不能にするためのランサムウェア及びマルウェアを使用する近時のグローバルなサイバー攻撃は、EU 内におけるサイバー回復性及び防護活動に更に力を入れるべき必要性を再認識させるものであった。デジタル単一市場の注記報告書の中でのべられているように、欧州委員会及び上級代表は、現在、とりわけ、2017 年 9 月に予定されたパッケージの採択による、2013 年のサイバーセキュリティ戦略の見直し行っている。その目的は、デジタル社会及びデジタル経済における信頼を増強し、これらの脅威に対するより効果的で部門横断的な対応を提供することになる。変化したサイバーセキュリティ生態環境の中におけるその役割を定めるため、ENISA すなわち EU ネットワーク情報セキュリティ局の任務も見直されることであろう。欧州理事会は、欧州委員会によるサイバーセキュリティ戦略の見直しの予定に賛成し

ている[1]。

2016 年 7 月にネットワーク情報サービス（NIS）指令[2]が採択されたことは、欧州レベルのサイバーセキュリティ回復性の構築へ向けた重要な歩みの 1 つであった。この指令は、サイバーセキュリティに関する EU 全域に適用される最初の規定を定め、サイバーセキュリティの能力を向上させ、そして、構成国間の協力を強化する。この指令はまた、重要な部門にある企業に対し、積雪な防護措置を講ずること、及び、関連する国内機関に対して重大なサイバーインシデントを通知することを求めている。これらの部門には、エネルギー、輸送、水道、医療、銀行及び金融市場インフラが含まれる。コンピューティングサービス及び検索エンジンであり得るオンライン市場は、同様の手立てを講じなければならなくなるであろう。異なる部門間を横断し、国境を横断する一貫性のある実装は、（2016 年に欧州委員会により設置された）ネットワーク情報サービス協力グループによって確保される。そのグループは、市場の細分化を回避する職務をもつ。この文脈において、ネットワーク情報サービス指令は、サイバーセキュリティの分野における全ての部門のための準拠枠組みであると考えられる。更に、この指令は、全ての関連する利害関係者を集めるコンピュータセキュリティインシデント対応チーム（CSIRT）を創設する。それと並行して、欧州委員会及び CERT-EU は、サイバー脅威の状況を積極的に監視し、そして、EU の機関の情報技術システムがサイバー攻撃に対して安全であり回復力をもつことを確保するために国内機関と情報を交換する。2017 年 3 月、WannaCry ランサムウェアのインシデントは、業務遂行上の情報交換及び助言の流通手段による協力に従事するための最初の機会をそのネットワークに提供した。EU コンピュータ緊急対応チームは、その脅威を解消し、かつ、被害者を支援するために、Europol にある欧州サイバー犯罪センター（EC3）、被害を受けた国のコンピュータセキュリティインシデント対応チーム（CSIRT）、サイバー犯罪部局及び産業界の主要なパートナーと密接に連絡をとった。この経験は、その後のインシデント（例：「NonPetya」）に対してネットワークがより良く準備することを可能にした。幾つかの検討課題が発見され、対処されつつある。

行動 12：欧州委員会は、構成国と連携して、ハイブリッドな脅威のサイバーな側面に対して利用者及びインフラをより良く保護するための技術を開発し、これをテストするため、サイバーセキュリティのための契約に基づく官民パートナーシップ合意の遂行過程の範囲内で、産業界と共に作業をする。

[1] 欧州理事会の 2017 年 6 月 22 日～23 日の決議

[2] Directive (EU) 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, OJ L 194, 19.7.2016, p.1.

2016 年 7 月、欧州委員会は、構成国と連携して、サイバーセキュリティのための官民パートナーシップ合意（cPPP）に、産業界と署名した。これは、サイバー脅威及びハイブリッドな脅威に対して利用者及びインフラをより良く保護するための技術を開発し、これをテストするために、EU の調査研究及び開発計画である Horizon 2020 に基づき、最大で 4 億 5000 万ユーロの投資をするものである。パートナーシップは、最初の汎欧州戦略研究アジェンダを発行した。そのアジェンダは、重要インフラ及び市民のサイバー攻撃に対する回復力の拡大に焦点を当てている。パートナーシップは、Horizon 2020 に基づいて資金付けられるサイバーセキュリティにおいて効率的かつ効果的に成果を得ることを導く利害関係者との連携を強化させた。パートナーシップは、情報通信技術のサイバーセキュリティ認証と関連する検討課題に関し、並びに、市場におけるサイバーセキュリティのスキルのある専門家の急激な不足といかに取り組むかに関し、並行して作業を進めている。民間の調査研究及び防衛において求められる高度の回復力を求める実質的な需要を考慮して、欧州防衛機関のサイバー研究及び技術グループは、欧州サイバーセキュリティ機関によってその戦略研究及び開発アジェンダの中で指定された調査研究領域に寄与している。

行動 13:欧州委員会は、構成国と協力して、ハイブリッドな脅威のサイバーな側面に対し利用者及びインフラをより良く防護するための技術を開発し、これをテストするため、契約によるサイバーセキュリティのための官民パートナーシップの遂行過程において、産業界と共に作業をする。

エネルギー部門において、欧州委員会は、NIS 指令の実装を強化するために、エネルギー専門家サイバーセキュリティプラットフォームの設置を伴うサイバーセキュリティに関する部門別戦略を準備しつつある。スマート計量システムのサイバーセキュリティのレベルを拡大するための最も利用可能な技術を検討した 2017 年 2 月のある研究結果は、このプラットフォームを支持する。欧州委員会は、Web ベースのプラットフォームである「EU インシデント及び脅威情報共有センター」も創設した。そのプラットフォームは、エネルギー部門におけるサイバー脅威及びサイバーインシデントに関する情報を解析し、共有する。

金融部門のハイブリッドな脅威からの回復力の増強

行動 14:欧州委員会は、ENISA[1]、構成国、関連する国際機関、欧州連合の機関及び国内機関並びに金融機関と協力して、脅威情報共有のプラットフォーム及びネットワークを促進し、かつ、そのような情報の交換の阻害要因に対処する。

[1] European Union Network and Information Security Agency

サイバー脅威が金融の安定に対するトップ脅威の中にあることを認識して、欧州委員会は、欧州連合内の支払サービスに関する規制枠組みを見直し、それは、現在、実装されている。改訂された支払サービス指令 [1]は、とりわけ、オンライン決済における不正行為を減少させるという目的により、支払手段の安全性を拡大し、顧客の本人確認を強化する新たな条項を導入した。この新たな立法枠組みは、2018 年 1 月に適用可能となる。現在、欧州委員会は、欧州銀行監督局の支援を受け、かつ、利害関係者と協議して、2017 年末を予定して、強力な本人確認及び決済トランザクションにおける安全性を運用名嚢なものとするための共有の安全な通信に関する規則上の技術基準を検討している。更に、国際的な場面においては、欧州委員会は、2016 年 10 月に G7 の財務大臣及び中央銀行総裁によって承認された「G7 金融部門におけるサイバーセキュリティの基本原則」に関し、関連する G7 のパートナーと密接な作業を行った。この基本原則は、（公的及び民間の）金融部門の組織のための策定されたものであり、増加するより巧妙なサイバー脅威を含め、サイバー脅威と共同で闘うための金融部門内における連携したサイバーセキュリティの取り組みに寄与するものである。

輸送

行動 15：欧州委員会及び上級代表は、（それらの関連する職務権限の範囲内で）構成国と連携して、ハイブリッドな脅威、とりわけ、輸送部門を横断するサイバー攻撃と関係するハイブリッドな脅威に対していかに対応するかを検討する。

EU 海上保安戦略行動計画 [2]の実装は、情報交換及び民間と軍当局との間の資産の共同利用についてのサイロに閉じこもるような気持ちを打破する助けとなるであろう。全政府のアプローチは、様々な当事者間の協力の強化を導いた。欧州委員会と EEAS の共同による民軍戦略研究アジェンダが 2017 年末までに完成され、重要海上インフラの保護に関する最終ワークショップが開催される予定となっている。この作業は、将来、海底パイプライン、エネルギー移転、光ファイバー及び在来の通信ケーブルに対して領海外からの干渉という新たな脅威に対応するために拡大され得る。

近時の研究報告 [3]は、沿岸警備の職務を行う国内機関のリスク評価能力を評価した。それは、

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, OJ L 337, 23.12.2015, p.35.

[2] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf 及び 2017 年 6 月 21 日に構成国に提示された EUMSS AP の実装に関する第 2 報告書

[3] 2017 年の「沿岸警備の職務を行う国内機関のリスク評価能力の評価」に関する研究報告書 https://ec.europa.eu/maritimeaffairs/documentation/studies <URL 一部省略>

共同活動をする上での最も重要な障壁を指摘し、そして、この特殊分野に関して EU レベル及び国内レベルで海上保安当局間の協力を拡大するための実際的な方法を勧告した。リスク評価は、海上保安上の脅威に対抗する際に重要であり、そして、ハイブリッドな脅威が付加的かつより複雑な検討を要するものであることから、ハイブリッドな脅威の評価及び防止に際しても、より有用なものである。この研究報告の結果は、主たる目的としてのハイブリッドな脅威に対する準備及び対応についてのこの分野における協力を強化するために、提案された勧告が評価され、実装され得るようにするため、沿岸警備と関連する異なるフォーラムに対して提示されることになるであろう。

テロリスト資金提供への対抗

行動 16:欧州委員会は、ハイブリッドな脅威への対抗に寄与するためにも、テロリスト資金提供に関する行動計画の実装を用いる。

ハイブリッドな脅威の加害者及び彼らの支援者は、彼らの計画を実行するための資金を必要とする。犯罪及びテロリスト資金提供に対する EU の治安に関する欧州アジェンダ及びテロリスト資金提供に関する行動計画に基づく取り組みは、ハイブリッドな脅威への対抗にも寄与し得る。2016 年 12 月、欧州委員会は、資金洗浄及び違法な現金支払の刑事制裁並びに資産の凍結及び没収を含む 3 つの立法提案を提示した [1]。

全ての構成国は、2017 年 6 月 26 日までに、第 4 次資金洗浄禁止指令 [2]を国内法化することを要する。また、2016 年 7 月、欧州委員会は、この指令を追加的な措置によって補充し強化することを狙った立法提案を送付した [3]。

2017 年 6 月 26 日、欧州委員会は、第 4 次資金洗浄禁止指令で予定されていた超国家的なリスク評価を発行した。欧州委員会は、第三国から違法に輸出された文化財の EU 内における輸入及び貯蔵を禁止するための規則案も提唱した [4]。今年後半、欧州委員会は、EU 内におけるテロリスト資金提供を追跡するための可能な追加的措置のために必要な欧州委員会が現在進めている評価に関して報告する。欧州委員会は、現金以外の支払手段の不正行為及び偽造行為と

[1] 効果的で真に安全な欧州連合に向けた進捗に関する第 3 次報告書(COM (2016) 831 final)
[2] 資金洗浄またはテロリスト資金提供のための金融システムの利用の防止、欧州議会及び理事会の規則(EU) No 648/2012 の改正、並びに、欧州議会及び理事会の指令 2005/60/EC 及び委員会指令 2006/70/EC の廃止に関する欧州議会及び理事会の 2015 年 5 月 20 日の指令 (EU) 2015/849（OJ L 141, 5.6.2015, p.73–117）
[3] 詳細については、効果的で真に安全な欧州連合に向けた進捗に関する第 3 次報告書(COM (2016) 831 final)及び同第 8 次報告書(COM (2017) 354 final)参照
[4] COM (2017) 26.6.2017, COM (2017) 340 final, SWD (2017) 275 final 0.

の闘いに関する立法の見直しもしている[1]。

効果的で真に安全な欧州連合に向けた進捗に関する第 8 次報告書は、テロリスト資金提供に対する行動計画の実装の状況に関し、より詳細な情報を提供する。

EU の共通の価値観及び包括的、開放的かつ回復力のある社会の促進

過激化及び暴力的な過激主義に対する回復力の構築

宗教上の過激主義及びイデオロギー上の過激主義、民族紛争及び少数派紛争は、特定のグループの支援により、または、グループ間の紛争を煽ることを通じて、国外の者によって扇動され得る。独立行動者からの脅威、移民の過程における潜在的な危機及び（移民に対する暴行を含む）極右の台頭並びに社会の分極化のリスクを含め、新たな過激化の経路の脅威のような、付加的な課題が生じた。過激化に関する作業を安全な欧州連合という文脈の中で進めながら、欧州委員会は、過激化に対して脆弱な人々がハイブリッドな脅威の加害者によって操作され得る限りにおいて、ハイブリッドな脅威という観点からも間接的に関係をもち得る。

行動 17:欧州委員会は、治安に関する欧州アジェンダに定める過激化に対する行動を実装しており、また、媒介者に対してネットワーク及びシステムを管理する際の適切な配慮を求め、違法なコンテントを除去するための手続を強化する必要性を解析している。

過激化の防止

欧州委員会は、暴力的な過激主義を導く過激化の防止の支援に関する 2016 年 6 月の通知に定めるとおり、社会内に取り込む教育及び共通の価値観の促進、オンラインの過激主義者のプロパガンダ及び刑務所内の過激化との闘い、第三国との協力の強化及び過激化の発展性をより良く理解するための調査研究の拡大、並びに、政策的な応答のより良き情報伝達のような重要な活動と共に、過激化に対する欧州委員会の多面的な対応の実装を継続している[2]。

過激化警戒ネットワーク（RAN）は、コミュニティレベルで地域の実務家と共働し、この分野において構成国を支援するための欧州委員会の作業の最前線に置かれた。より詳細な情報は、効果

[1] 効果的で真に安全な欧州連合に向けた進捗に関する第 8 次報告書(COM (2017) 354 final)

[2] http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf

的で真に安全な欧州連合に向けた進捗に関する第 8 次報告書[1]の中で提供される。

オンラインの過激主義及びヘイトスピーチ

治安に関する欧州アジェンダに沿って[2]、欧州委員会は、とりわけ、Europol の EU Internet Referral Unit 及び EU Internet Forum を介して、オンラインの違法なコンテントの可用性を減少させるための手立てを講じた[3]。オンラインの違法なヘイトスピーチに対抗する行動準則[4]に基づき、大きな進呈が得られた。より詳細な情報は、効果的で真に安全な欧州連合に向けた進捗に関する第 8 次報告書の中で提供される[5]。欧州理事会の決議[6]、G7 サミット[7]及びハンブルグ G20 サミット[8]に照らしても、これらの行動が強化されることになるであろう。

オンラインのプラットフォームは、違法なコンテントまたは潜在的に危険なコンテントとの闘いにおいて、重要な役割をもつ。中期見直しに定めるように[9]、デジタル単一市場戦略に基づき、欧州委員会は、違法なコンテントの除去のための仕組み及び技術上の解決策に焦点を当てたプラットフォーム対話のより良き連携を確保する。それが適用可能なときは、その目的は、違法なコンテントの通知及び削除のような側面に関するガイダンスによって、これらの仕組みを下支えとすべきである。欧州委員会は、法的責任の法令に関するガイダンスも提供する。

第三国との協力の強化

行動 18：上級代表は、欧州委員会と連携して、近隣国の領域においてハイブリッドリスクの調査を開始する。上級代表、欧州委員会及び構成国は、それぞれの処理の際、パートナー国の能力を構築し、かつ、ハイブリッドな脅威に対するそれらの回復力を強化するために、法律文書を用いることになる。相手国の能力の拡大についてパートナー国を支援するために、EU の機関とは別に、または、EU の機関を補充するものとして、CSDP ミッションが配置され得る。

欧州連合は、就中、安全保障と開発との間の関連の上に構築すること、海底された欧州近隣国

---

1 COM(2017) 354 final
2 詳細については、第 8 次報告書(COM (2017) 354 final)参照
3 詳細については、第 8 次報告書(COM (2017) 354 final)参照
4 Code of Conduct on illegal online hate speech, 31 May 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
5 詳細については、第 8 次報告書(COM (2017) 354 final)参照
6 Council Conclusions 22-23 June 2017.
7 G7 summit in Taormina, Italy, 26-27/05/2017.
8 G20 summit in Hamburg, Germany, 07-08/07/2017.
9 上述の委員会通知 COM (2017) 228 final 参照

政策の安全保障の場面を開発すること、並びに、地中海周辺諸国と対テロリズム及び安全保障の対話を開始することによって、安全保障部門において、パートナー諸国における能力及び回復力の構築にその焦点を当てることを強化してきた。その範囲内で、モルドバ共和国との協力により、パイロットプロジェクトのリスク評価が開始された。その目的は、その国の主要な脆弱性の検討を支援すること、及び、EU の支援が特にこれらの領域に狙いを定めることを確保することである。パイロットプロジェクトの結果は、調査それ自体としては有用であるとみなされるということを示した。得られた経験に基づき、欧州委員会及び EEAS は、有効性の構築、戦略的通信、重要インフラの防護及びサイバーセキュリティとの見出しの下に、行動の優先順位をつけるための勧告を行うであろう。

今後、追加的な近隣諸国は、この調査から、国によって異なるローカルな事情と特定の脅威を反映する個別の適応ではあるが、この最初の経験に基づいて構築され、進行中のテロリズムへの対抗策と安全保障上の対話の重複を避ける利益を受けることができるであろう。より一般的には、2017 年 6 月 7 日、欧州委員会及び上級代表は、「EU の対外活動における回復性への戦略的取り組み」に関する共同通知 [1]を採択した。その目的は、今日のグローバルな課題に対してより回復性をもつようになることについて、パートナー国を支援することである。欧州委員会は、期待、防止及び準備を強調し、危機の封じ込めから、より構造的で、長期にわたる、脆弱性への取り組みへと移行すべき必要性を認識している。

発展のためのサイバー回復力

EU は、それらの国々の情報ネットワークの回復力を強化するため、欧州の領域外の国々を支援している。サイバー攻撃は国境というものを知らないので、無限に拡大し続けるデジタル化は、情報ネットワークシステムの回復性に対する特別の課題をグローバルにもたらすというセキュリティ上の内在的な特性をもっている。EU は、偶発的な失敗及びサイバー攻撃を防止し、これにタイプするためのそれらの国々の十分な能力を構築するため、第三国を支援している。2016 年に完了したマケドニア旧ユーゴスラビア共和国、コソボ [2]及びモルドバにおけるパイロットサイバーセキュリティプロジェクトの後、欧州委員会は、2017 年から 2020 年にかけ、主としてアフリカ及びアジア、加えて、ウクライナにおいて、第三国のサイバー回復力の拡大のための新たな計画を開始する。この計画は、人権及び法の支配を遵守する全政府のアプローチに基づき、第三国における

[1] Joint Communication to the European Parliament and the Council: A Strategic Approach to Resilience in the EU's external action JOIN (2017) 21 final.

[2] この表示は、地位に関する意見書を妨げるものではなく、UNSCR 1244 及びコソボの独立性に関する宣言に関する ICJ 意見書に沿うものである。

重要情報インフラ及びネットワークの安全性及び準備の向上を目的とする。

航空の安全性

民間航空は、テロリストにとって、依然として重要かつ象徴的な標的であり続けているが、ハイブリッドなキャンペーンの一部としても標的とされ得る。EU は、頑健な航空安全の枠組みを構築したが、第三国から出発する航空機は、より脆弱なものであり得る。国連安全保障理事会決議 2309 号（2016 年）に沿って、欧州委員会は、第三国における能力を構築するための取り組みに更に力を入れている。2017 年 1 月、欧州委員会は、EU 及び構成国のレベルで、並びに、国際的なパートナーと共に行われる能力構築の取り組みの優先順位及び連携を確保するための新たな統合されたリスク評価を開始した。2016 年、欧州委員会は、民間航空機に対するテロリズムの脅威に対抗するため、アフリカ及びアラビア半島における民間航空の安全性に関する 4 か年プロジェクトを開始した。このプロジェクトは、パートナー国の間における専門知識の共有、並びに、人材育成、訓練及び指導活動をする欧州民間航空会議構成国からの専門家の共有に焦点を当てている。この活動は、2017 年中にその規模が拡大される。

C. 危機の防止、危機への対応及び復旧

生じた結果は、国内レベル及び EU レベルの長期的政策によって解消され得るが、短期的には、迅速かつ連携した方法で、ハイブリッドな脅威を防止し、それに対応し、それから復旧するための構成国及び欧州連合の能力を強化することは、依然として重要なことである。ハイブリッドな脅威によって惹起される出来事に迅速に対応することは、重要なことである。昨年、この分野において、現在ではハイブリッドな攻撃が発生する際の危機管理プロセスを EU が割り当てる中で位置付けられている業務遂行手順と共に、多数の進展があった。今後、定期的な監視及び演習が行われる。

行動 19：上級代表及び欧州委員会は、構成国と連携して、共通の業務遂行手順を定め、危機管理及び統合された政治的危機対応手続の上の構築される複雑でハイブリッドな脅威に対する対応における戦略的な意思決定を向上させるために、定期的に演習を実施する。

共同枠組みは、EU 内の対応の仕組み [1]及び早期警戒システムを統括するために、ハイブリッド

[1] 理事会の EU 統合政治危機対応協定(IPCR)、委員会の ARGUS システム及び EEAS の CRM

な脅威によって惹起される出来事に対する迅速な対応をする仕組みの構築を勧告した。この目的のために、欧州委員会の機関及び EEAS は、ハイブリッドな脅威に対抗するための EU の業務遂行手順（EU 作戦書）[1]を発行した。それは、統括のための様式、諜報の融合及び解析、情報政策決定過程、演習及び訓練、並びに、ハイブリッドな脅威発生時におけるパートナー組織との連携、特に NATO との連携を示すものである。同様に、NATO は、サイバー防衛、状況認識及び危機管理の分野におけるハイブリッドな脅威の防止及び対抗の上での NATO-EU 間の交流拡大のための作戦書を作成した。EU 作戦書は、NATO との交流を含む欧州連合同時統合演習の一部として、2017 年秋の演習を通じてテストされる。

行動 20：欧州委員会及び上級代表は、それぞれの職務権限を有する領域において、広域的かつ深刻にハイブリッドな攻撃が発生した場合において、TFEU の第 222 条及び TEU の第 42 条第 7 項の適用可能性及び実務上の意味を検討する。

TEU の第 42 条第 7 項は、構成国の領土上における武力侵略を指示し、他方で、TFEU の第 222 条（連携条項）は、構成国の領土上におけるテロリスト攻撃または自然災害もしくは人為的な災害を指示している。後者は、犯罪活動と破壊活動の混合であるハイブリッドな攻撃の場合において、より使用され得るものである。連携条項が用いられることは、理事会レベルにおける統括（統合政治危機対応協定 IPCR）、EU の関連する機関、部局及び組織の関与、並びに、EU を支援する計画及び仕組みが発動される契機となるものである。理事会決定 2014/415/EU は、連携条項の欧州連合による実装のための準備を定めている。その適用の様式は、現在においてもなお有効であり、そして、この理事会決定を改正すべき必要性は存在しない。ハイブリッドな攻撃が武力侵攻を含んでいる場合、第 42 条第 7 項も呼出される。そのような場合、補助及び支援は、構成国及び EU の両者から提供される。欧州委員会及び上級代表は、そのような攻撃に対応するための最も効果的な方法の評価を継続している。

上記に述べた EU の業務遂行手順の採択は、この評価を直接に支援するものであり、かつ、2017 年 10 月の EU 同時統合演習（PACE）の一部として吟味されることになる。この演習は、ハイブリッドな脅威によって惹起された曖昧さが明確性を損ねるような場合における迅速な意思決定を目標として、EU の様々な仕組みや権能が関係することになる。

行動 21：上級代表は、構成国と連携して、共通安全保障及び防衛政策の範囲内において、ハイブリッドな脅威に対抗する軍事行動の能力を統合し、活用し、そして、統括する。

[1] 2016 年 7 月 7 日に採択された Staff Working Document (2016) 227

CFSP/CSDP を支援する統合軍事能力のための職務遂行に対応して、2016 年 12 月の軍事専門家とのセミナー及び 2017 年 3 月の欧州連合軍事委員会作業部会からのガイダンスの後、「CSDP 内におけるハイブリッドな脅威に対抗するための EU の軍事的寄与」に関する軍事上の助言が 2017 年 7 月に完了した。これは、概念開発実装計画を通じて、更に先に進められる。

D. EU と NATO の協力

行動 22：上級代表は、欧州委員会と連携して、NATO との間において、それぞれの組織上の意思決定過程の一体性の原則及び自律性の原則を尊重しつつ、状況認識、戦略的な通信、サイバーセキュリティ、及び、ハイブリッドな脅威に対抗するための「危機回避及び危機対応」に関し、非公式の対話を継続し、かつ、強力及び連携を拡大する。

2016 年 6 月 8 日にワルシャワにおいて、NATO の事務総長と共に、欧州理事会議長及び欧州委員会によって署名された共同宣言に基づき、EU 及び NATO は、実装を求める 42 の提案の共通のセットを作成した。それは、その後、EU 及び NATO 理事会の双方によって、2016 年 12 月 6 日、それぞれ同時に行われた手続の中で、承認された [1]。2017 年 6 月、上級代表の副議長及び NATO の事務総長は、共同宣言の 42 の行動に関して行われた全体的な進捗状況に関する報告書を発行した。ハイブリッドな脅威への対抗は、共同宣言中で指定された 7 つの協力分野の 1 つであり、42 の行動の中の 10 を数える。この報告書は、過去 1 年に行われた共同の取り組みが大きな成果をあげたことを示している。ハイブリッドな脅威に対抗するための欧州研究拠点、より良い状況認識、EU Hybrid Fusion Cell の設置及びこの機関と新設された NATO ハイブリッド分析部門との交流、並びに、戦略的通信チーム間の共同活動を含め、ハイブリッドな脅威への対抗を目的とする特定の行動の多くについては、既に述べたとおりである。NATO の職員及び EU の職員は、初めて、ハイブリッドなシナリオへの彼らの対抗を共に演習することになるであろう。この演習は、共通提案の 3 分の 1 以上の実装をテストすることが期待されている。EU は、今年、EU 自体の同時進行的で連携した演習を行い、そして、2018 年には主動的な役割を果たすことになる。

回復性に関し、EU の職員及び NATO の職員は、共に、EU の統合政治危機対応の仕組み上のものを含め、クロスブリーフィングを実施した。NATO のワークショップによるもの、または、欧州防衛機関の運営委員会への参加を含め、NATO の職員及び EU の職員間の定期的な接触は、国内の回復力のための NATO のベースラインの要求事項に関する情報交換をすることができるようにした。回復力強化に関する欧州委員会及び NATO 間の別の情報交換が、この秋に計画さ

[1] http://www.consilium.europa.eu/en/press/press-releases/2016/12/06-eu-nato-joint-declaration/

れている。EU-NATO 連携に関する次の進捗状況報告書は、この 2 つの組織の間の協力拡大の可能性を示唆することになるであろう。

3. 結論

共同枠組みは、ハイブリッドな脅威への対抗を支援し、そして、EU レベル及び国内レベルにおける回復力並びにパートナーのための回復力を育成するために指定された行動の概要を示す。欧州委員会及び上級代表は、全ての分野にわたって構成国及びパートナーと密接に猟力して職務を遂行しているが、現時点でも発生し続けるハイブリッドな脅威に直面し、このような協力体制が維持されることが重要である。構成国は、国家安全保障及び法の支配の維持と関連するハイブリッドな脅威に対抗する第一次的な責任をもつ。国内の回復力及びハイブリッドな脅威に対する防護のための集中的な取り組みは、同様の全体的な取り組みと相互に強化し合う要素として理解されなければならない。それゆえ、構成国は、脆弱性の範囲及び全欧における準備状況に関する重要な情報を提供するため、可能な限り速やかに、ハイブリッドなリスクの調査を実施することが推奨される。認識の向上における大きな進展の上に構築されるものとして、EU Hybrid Fusion Cell の能力は、極大化されなければならない。上級代表は、ハイブリッドな脅威の発生により効果的に対抗するための StratCom Task Forces の職務を支援するために、構成国を招請する。EU は、フィンランドが牽引するハイブリッドな脅威の対抗のための欧州拠点を完全に支援することになるであろう。

EU は、既存の法律文書及び計画の広い幅に依拠し、その回復力を構築するための構成国及びパートナーを支援することに大きな力を入れている。輸送、エネルギー、サイバーセキュリティ、重要インフラ、違法な利用からの金融システムの保護、並びに、暴力的な過激主義及び課猥下に対抗するための取り組みのような領域においては、回復力を構築するための行動の中で、大きな進展が得られた。ハイブリッドな脅威の性質は進化するものであるので、回復力を構築する EU の行動は、継続されることになるであろう。とりわけ、EU は、関連部門におけるハイブリッドな脅威に対する重要インフラの防護及び回復力の向上のための指標を開発する。

欧州防衛基金は、構成国と共に、ハイブリッドな脅威に対する回復力を強化するための優先事項に共同して拠出することができる。予定されているサイバーセキュリティパッケージ、並びに、ネットワーク情報セキュリティ指令の実装を目的とする部門横断的な措置は、EU 全域におけるハイブリッドな脅威と対抗するための新たなプラットフォームを定めることになるであろう。

欧州委員会及び上級代表は、構成国及び利害関係者に対し、それが必要な場合には、速やかに合意に至ること、そして、この通知に概要を示した回復力の強化を目的とする多数の措置の迅速かつ効果的な実装を確保することを求める。EU は、NATO との既に実り多い協力に基づき、

更にそれを深化させることになるであろう。

欧州連合は、複雑なハイブリッドな脅威に対応するために、EU の関連法律文書を動員する作業を続けている。構成国の取り組みを支援することは、そのコアパートナーと共により強力でより多くの責任を果たし得る安全の提供者として行動する欧州連合にとって、優先事項の 1 つであり続ける。