ハイブリッドな脅威報告書 JOIN(2018) 14 final

[参考訳]

2018 年 11 月 14 日
明治大学法学部教授
夏　井　高　人

＊＊＊

Joint Report to the European Parliament, the European Council and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018, JOIN(2018) 14 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:52018JC0014&from=EN
[2018 年 10 月 6 日確認]

共同報告書 JOIN(2018) 14 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または電磁波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型の脅威への対応策に関する政策文書である。

共同報告書 JOIN(2018) 14 final は、「Joint Framework on countering hybrid threats: a European Union response」（JOIN(2016) 18 final）に定めるハイブリッドな脅威に対抗するための行動計画 1～行動計画 22 に対応して、各行動計画について、現時点までの達成状況を踏まえ、問題点を指摘し、今後の方向性を示している。

共同報告書 JOIN(2018) 14 final は、本文のみで構成されている。この参考訳においては、共同報告書 JOIN(2018) 14 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、あくまでも共同報告書 JOIN(2018) 14 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。

共同報告書 JOIN(2018) 14 final と関連する最新の文書として、安全の欧州連合第 16 次進捗状況報告書（COM(2018) 690 final）が 2018 年 10 月 10 日付けで公表されている。

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0690:FIN
[2018 年 11 月 9 日確認]

共同報告書 JOIN(2018) 14 final の「行動 3」に関する報告の中で西バルカン諸国の国家機関に関して言及されている指摘は、そのまま日本国の国家機関及び地方自治体の機関にもあてはまるものであると考えられる。

この点に関して、かなり巨大な脆弱性が存在している。そのことは、個人データの安全性確保との関係においても深刻な影響を与え続けている。

事実の問題として、日本国のサイバーセキュリティ戦略は、現実に幾つかの深刻な事態が発生した際に、大きく改善されたと評価できる。しかし、まだ十分なものではない。特に、一般的な刑法犯の背後にあるサイバーセキュリティの脅威に関する認識に大きく欠ける点がある。これは、省庁間の情報共有及び意思決定が正常に機能していないことに起因するものと推測される。

しかし、窃盗、横領、背任、汚職のような古典的かつ比較的素朴な刑法犯は、（そもそもその監視及び摘発がかなり緩慢であることを一応措くとしても）より高度で現代的な情報犯罪の手口、練習、訓練の一種として、または、関連当局の反応を観察するための行為の一種として実行されていることがあり得るのである。この場合、当該実行者は、実質的にみて、本来の目的との関係において間接正犯の道具的な立場で刑法犯に属するごく普通の犯罪行為を実行していることがあり得る。それゆえ、表面的な犯罪行為の摘発だけで満足してしまうことは、ものごとの本質に気づかない最大の原因となり得る。このことは、事務委託を受ける民間企業等においては、より深刻なものであることがあり得る。

政策論全体としてみた場合、（名目 GDP の拡大を含め）目先の短期的な経済的利益または金銭的利益のみに目を奪われることなく、中期的または長期的な視点から、安定した堅牢な防護を構築・維持・拡大するためのサイバーセキュリティ基本政策の根幹部分の更なる練り直しが必要である。

同様に、外見上では単なる投資に見える行為のような、それ自体としては犯罪行為ではない適法な取引の一種である行為がハイブリッド脅威に該当する場合（特に、外国政府及び関連企業等による EU の重要インフラや重要施設等の買収の場合等）を示唆し、そのような脅威に対抗するための法案の審議が行われている（共同報告書 JOIN(2018) 14 final の「行動 5」参照）。ここ文脈で示されている重要な資産に対する外国からのハイブリッド脅威に該当する影響力を排除し得る国家制度の存否は、GDPR に基づく個人データの第三国移転との関係においても一定の意味をもち得るものであり、特に重要な情報、データまたはシステムへのアクセスの可否に関して留意しなければならない。

一般に、ハイブリッドな脅威は、進化を続けており、現時点において既に、虚偽情報（disinformation）の脅威を含め、共同報告書 JOIN(2018) 14 final に示されているよりもはるかにハイブリッドである。

EU の防衛政策全体に関しては、「European Defence Action Plan」（COM(2016) 950 final）が参考になる。海事、洋上防衛及び海上国境管理に関しては、「European Union Maritime Security Strategy (EUMSS) - Action Plan」（Brussels, 16 December 2014）、「For an open and secure global maritime domain: elements for a European Union maritime security strategy」（JOIN(2014) 9 final）、「Migration on the Central Mediterranean route Managing flows, saving lives」（JOIN(2017) 4 final）が参考になる。欧州司法裁判所の関連判例として、*European Parliament* v *Council of the European Union*, Case C-658/11, 24 June 2014, OJ C 292, 1.9.2014, p.2-3 がある。

共同報告書 JOIN(2018) 14 final の「行動 5」の中において「the European Directive on the Protection of Critical Infrastructure」として示されている指令とは、理事会指令 2008/114/EC（OJ L 345, 23.12.2008, p.75-82）のことを指す。その関連文書として、委員会スタッフ作業文書 SWD(2013) 318 final がある。

共同報告書 JOIN(2018) 14 final の「行動 6」の中において「the Security of Gas Supply Regulation」として示されている規則とは、規則(EU) 2017/1938（OJ L 280, 28.10.2017, p.1-56）のことを指す。この規則における「security」の定義は、第 2 条(1)において指令 2009/73/EC（OJ L 211, 14.8.2009, p.94-136）の定義を参照するのみである。そして、同指令の第 2 条(32)は、「‘security’ means both security of supply of natural gas and technical safety」と定義しているから、この「security」が天然ガスの物的な供給の安全性だけではなく、天然ガスプラント及び供給網の管理のための情報システムのセキュリティを含むものであることが明らかである。

また、共同報告書 JOIN(2018) 14 final の「行動 6」の中にある「the Risk Preparedness Regulation」とは、COM (2016) 862（2016/0377/COD）によって提案されているリスク対応準備規則案のことを指す（2018 年 11 月 10 日現在、審議中）。日本国の法令中において、同規則案に相当する法令は存在しない。

共同報告書 JOIN(2018) 14 final の「行動 7」にある海上交通及び海上輸送におけるハイブリッド脅威の状況認識は、日本国においては極めて希薄である。これは、海事法の分野が防衛法や警察法の分野と隔絶された超然たる立場を維持してきたことに起因するものである。少なくとも、海事取引法だけに限定する領域設定は全廃または禁止し、全法学分野を横断するものとして、公法と私法を全く区別しないものとして、海事法そのものを根本的に再構築しなければならない。一般に、法学理論の分野における公法と私法との区分は、単に無意味というだけではなく、かなり有害なものとなりつつある。

日本国においては、共同報告書 JOIN(2018) 14 final の「行動 10」にあるような民間病院等を含む CBRN リスクに対処するための官民を通じた国家規模の総合演習が実施されたことはなく、そのための法制も官民の情報共有システムも訓練制度も全く存在しない。日本国においては、現代の CBRN リスクに対する官民を通じた国家的準備が存在しないと言える。それゆえ、例えば、仮に 2020 年のオリンピックにおいて CBRN 攻撃が実行される可能性が皆無ではないにも拘らず、スポーツ競技関連団体は、それ自体としても、政府、自衛隊、警察及び医療機関との連携等に関しても、実質的にはほぼ何の準備も訓練もしていない。

そもそも、一般に、大学教員を含め、日本国のスポーツ関係の専門家の圧倒的多数は、CBRN 及びハイブリッド攻撃の際の危機管理に関する教育や訓練を受けておらず、関連専門知識を欠いているのが普通である。日本国の領土上に居住または滞在する全ての者は、CBRN リスクの前に素っ裸で立たされているのと同然の状況にある。その意味において、日本国は、EU との関係においては、高リスク第三国の一種である。

あくまでも一般論であるが、スポーツ法学の分野においては、プロとアマを区別することなく、スポーツ参加者の身体生理学や救命措置、これらの予防・対処に必須のものとなる契約・保険、合理性のない練習の強制・競技会参加の強制に対する刑事制裁、スポーツ関連団体に対する行政規制、麻薬及びドーピングのような薬物規制、賭博及び八百長のような行為に対する刑事制裁、公路における競技会実施の際の交通規制及びドローン規制、電波の輻輳または枯渇対応の通信法制と連携する競技会

運営方針の規律等を含む他の基本的な事項並びに必要な比較法研究に加え、（競技場や練習場等の多衆が集合する蓋然性の高い場所における全ての類型の物理攻撃が十分に予想されることから）CBRN 対応及び（競技の測定、結果の計算等を含む情報システムへの介入や破壊行為が十分に想定されることから）サイバー攻撃対応の基本的な素養と訓練も必須のものとなっていると考える。更に、電磁波（EMP）攻撃の可能性も想定しなければならない。

共同報告書 JOIN(2018) 14 final の「行動 16」にある「第 5 次資金洗浄禁止指令（the 5th Anti-Money Laundering Directive）」とは、指令(EU) 2018/843（OJ L 156, 19.6.2018, p.43-74）による改正後の指令(EU) 2015/849（OJ L 141, 5.6.2015, p.73-117）のことを指す。

共同報告書 JOIN(2018) 14 final の「行動 17」にある「High-Level Expert Group on Radicalisation」の 2018 年 5 月 18 日の最終報告書は、本文、別紙及び「Illustration of the ongoing work contributing to the implementation of HLCEG-R recommendations」によって構成された文書であり、下記の Web サイト上で公表されている。

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180613_final-report-radicalisation.pdf
[2018 年 11 月 13 日確認]

共同報告書 JOIN(2018) 14 final の「行動 18」にある「Hybrid Risk Surveys」に関しては、共同スタッフ作業文書 SWD(2017) 227 final の中でより詳しく述べられている。

共同報告書 JOIN(2018) 14 final の「行動 18」にある「Commission's Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks」とは、COM(2017) 610 final のことを指すと解される。

共同報告書 JOIN(2018) 14 final の「行動 19」にある「joint staff working document in June 2016」とは、2016 年 7 月 7 日に採択された Staff Working Document (2016) 227 のことを指す。また、「行動 19」の中で述べられている EU の危機管理体制に関しては、委員会勧告(EU) 2017/1584（OJ L 239, 19.9.2017, p.36-58）の中で述べられていることを十分に理解する必要がある。

共同報告書 JOIN(2018) 14 final の「行動 20」にある TFEU 第 222 条は、構成国がテロリスト攻撃の対象とされ、または、自然災害もしくは人為的災害（man-made disaster）の被害を受けた場合において、連携の精神（a spirit of solidarity）により、軍事行動を含む共同活動を実施する法的根拠を定めている。同条の解釈に従い、EU の政治思想上の基礎である民主主義に基づく社会を破壊することを目的とする場合、その目的を達成するための手段としての物理攻撃、サイバー攻撃及びハイブリッドな攻撃は、テロリスト攻撃の範疇に含められ得る。

EU の構成国に対する第三国のハイブリッド攻撃における対外的対応には、軍事行動だけではなく、交渉及び制裁を含めた外交活動も含まれ得る。

共同報告書 JOIN(2018) 14 final の「行動 21」においては、EU と NATO の参謀部レベルの連携の際に、個人データ保護法令を尊重する旨を述べている。EU の参謀部には規則(EC) No 45/2001 が適用される。しかし、軍事における個人データ保護の具体的内容に関しては、不明な部分が圧倒的に多い。

共同報告書 JOIN(2018) 14 final の「行動 22」にある EU 全体としての危機管理体制に関しては、委員会勧告(EU) 2017/1584 の中で述べられていること及び EU の危機管理関連法令を十分に理解した上で考察する必要がある。

（この参考訳を作成するに際し考慮した事項）

「European Defence Agency」は、一般に、「欧州防衛機関」と訳されている。しかし、「European Defence Agency」は、TFEU 付属議定書第 10 号の第 1 条(a)及び TEU 第 46 条第 2 項に定める EU の「Agency」であって、EU の「Institute」ではないので、「Agency」を「機関」と訳すのは、明白な誤謬である。

この参考訳においては、「European Defence Agency」を「欧州防衛局」と訳すことにした。

なお、「International Atomic Energy Agency」は、EU の部局（Agency）ではないので、慣例に従い、「国際原子力機関」と訳すことにした。

また、「Single Analytical Intelligence Capability（SAIC）」は、従前の参考訳においては「単一情報分析機関」と訳した。しかし、「Single Analytical Intelligence Capability」は、EU 軍事参謀部（EU Military Staff）の部局の 1 つである。そのことから、この参考訳においては、「Single Analytical Intelligence Capability」を「単一情報分析部」と訳すことにし、従前の訳を一括して改める。

「Connecting Europe Facility」は、多数の関連文書を検討した上で、「欧州接続機能」と訳すのが最も妥当であると判断し、そのように訳すことにした。

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、後掲ハイブリッドな脅威報告書 JOIN (2017) 30 final の参考訳、後掲ハイブリッドな脅威通知 JOIN(2018) 16/final の参考訳、後掲安全の欧州連合第 15 次進捗状況報告書 COM/2018/470 final の参考訳、委員会勧告(EU) 2017/1584 の参考訳、ENISA 規則(EU) No 526/2013 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通知 JOIN(2018) 16/final の参考訳は、法と情報雑誌 3 巻 9 号 281～295 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。安全の欧州連合第 15 次進捗状況報告書 COM/2018/470 final の参考訳は、法と情報雑誌 3 巻 10 号 101～122 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。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。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。

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) 2016/1624 の参考訳は、法と情報雑誌 2 巻 6 号 1～98 頁にある。指令(EU) 2018/843 による改正後の指令(EU) 2015/849 の参考訳は、法と情報雑誌 3 巻 8 号 276～328 頁にある。

規則(EC) No 45/2001 の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 111～146 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のほか、大沢秀介・荒井誠・横大道聡編『変容するテロリズムと法－各国における＜自由と安全＞法制の動向』（弘文堂、2017）、植月献二「EU における原子力の利用と安全性」外国の立法 244 号 39～55 頁（2010）、八田達夫・池田真介「欧州 TSO による調整電力市場と送電権市場の運用状況調査: 日本における電力改革への示唆」独立行政法人経済産業研究所 (2018)、三菱総合研究所「平成 25 年度安全保障貿易管理対策事業（安全保障貿易管理影響実態調査）調査報告書」（2014 年 2 月 28 日）、同「海外食品安全機関の動向に関する調査報告書」（平成 23 年 3 月）、Maria Mälksoo, Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO, European Security Vol.27, Issue 3, pp.374-392 (2018)を参考にした。

＊＊＊

2017 年 7 月から 2018 年 6 月までの間における ハイブリッドな脅威への対処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、欧州理事会及び理事会宛共同報告書 JOIN(2018) 14 final

イントロダクション

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）[1]は、ハイブリッドな脅威に対する欧州連合の活動の中心にある状況認識、回復力及び対応について述べている。早い段階で不正なハイブリッド活動を検知し、理解するための我々の能力を向上させること、そして、（例えば、輸送、通信、電力及び金融のような）我々の社会及び機関の重要インフラの回復力を拡大することは、攻撃に耐え、回復させるための我々の能力を向上させるための基本となるものである。ハイブリッドな脅威に対抗するためには、構成国の活動と欧州の機関の活動を要する。共同枠組みの中で指示された 22 の行動計画に関する最初の報告書[2]は、理事会に対し、2017 年 7 月 19 日に提出された。この 2018 年版報告書は、昨年夏以降の進捗状況の概要を提供する。

4 つの優先的な行動分野の全てにおいて、大きな進捗があった。

- 状況認識の向上
- 回復力の構築
- 危機の予防及び対応、並びに、迅速かつ調整された回復のための構成国及び欧州連合の能力の強化
- 措置の補完を確保するための NATO との協力拡大

脅威のハイブリッドな性質の認識

行動1：構成国は、ハイブリッドリスク調査を開始すべきである

作業を進めるため、理事会によって、輪番制の議長国が議長となる議長の友グループが設置された。2017 年 12 月、構成国は、ハイブリッドな脅威に対する構成国の重要な脆弱性を評価するための調査を開始した。構成国の対応に基づき、議長国は、2018 年末前にコレペールに対し、報告書を提出する見込みである。

グループの任務が 2018 年 6 月末に終了することに鑑み、議長の友グループは、その 4 月の会合において、議長国の提案に基づく将来の任務に関する討議を開始した。これは、現在の任務を 2020 年まで延長し、かつ、その内容を拡大するものである：すなわち、構成国の準備及び回復力を強化するための選択肢を分析すること、国内の発展を注視し、ハイブリッド分野の政策調整を支援し、ハイブリッド脅威への対抗の分野における EU と NATO 間の協力に関する理事会の仕事を支援すること、そして、

[1] JOIN (2016) 18 final.

[2] 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) 30 final.

ハイブリッド脅威に関し、情報交換し、共通理解を発展させることである。

EU の対応の組織化:認識の向上

行動2 :EU Hybrid Fusion Cell の創設

EU の民間/軍単一情報分析部の一部として EU 情報状況センター内にある EU Hybrid Fusion Cell は、民間及び軍の分析担当者と構成国の諜報当局及び公安当局の貢献の両者を用いている。それは、2017 年 7 月に全面的な運用能力を達成し、2017 年の NATO との間の同時統合演習(PACE17)の間にその立場が確認された。EU Hybrid Fusion Cell は、機密情報及び広範な利害関係者からのハイブリッド脅威に関するオープンソース情報を受け取り、それを分析する。そして、その判断を情報提供するため、EU の期間及び構成国の全体の中で報告及び分析結果が共有される。現在に至るまでの間、EU Hybrid Fusion Cell は、ハイブリッドな脅威に関する 100 を超える成果物を出した。CERT-EU(EU の機関のコンピュータ緊急対応チーム)は、発生しつつあるサイバー脅威または現在進行中のサイバー脅威に関する情報を共有することにより、EU Hybrid Fusion Cell の仕事に貢献する。しかしながら、化学兵器、生物兵器、放射線兵器及び核兵器の分野において、サイバー及び防諜の特別の専門知識は、現在のところ限定的なものである。

その仕事を増幅するため、EU Hybrid Fusion Cell は、国内連絡部局のネットワークを構築した。現在までの間に、28 の構成国中の 26 の構成国が EU Hybrid Fusion Cell との間でその専門知識を共有するために継続的に会合するための担当部局を指定した。

更に、このネットワークは、このネットワークと均等なものであり、様々な回復活動に対応する伝達に焦点を当てた EEAS 委員会の共同ネットワークによってミラーされる。これらの会合は、輸送、インフラ、電力、サイバーセキュリティ及び敵対的諜報活動を含むテーマ別の問題に焦点を当てて、月次で開催される。

戦略レベルにおいて、EU Hybrid Fusion Cell は、ワークショップ、演習に参加することにより、及び、ハイブリッド脅威に対抗する能力を構築するための課題に関する日々の討議を介して、ヘルシンキにあるハイブリッド脅威への対抗の欧州研究拠点との関係を発展させつつある。

共同宣言の枠組みの下において、スタッフ対スタッフの NATO ハイブリッド分析部門の業務への従事が日々行われている。2017 年 9 月、ハイブリッド課題に関する画期的な同時統合評価が公表され、2018 年に提供が予定されている成果物は、南部近隣国及び東部近隣国から発生しているハイブリッドな検討課題に焦点を当てることになるであろう。

行動 3:戦略的通信

戦略的通信は、能力を開発する多数の異なる関係者との間で、EU における付加的なモメントを獲得した。2018 年 4 月 26 日の通知「オンライン虚偽情報の追跡:欧州のアプローチ」[3]は、虚偽情報をハイブリッドな脅威の 1 つとして認識し、欧州委員会、欧州対外行動局及び構成国の間における強化されたネットワークを含め、多数の行動を定めた。2015 年 3 月の欧州理事会の命令により創設された東部

[3] COM(2018)236 final.

Stratcom タスクフォースの有益な経験は、共同通知「ハイブリッド脅威との直面：欧州人の保護」[4]の中で提案されているように、強調され、かつ、強化される必要がある。

東部 Stratcom の仕事の大半は、主として東部パートナーシップ領域及びロシアにおける EU の派遣団を支援すること、国内監視または領域監視の活動範囲を拡大することに焦点を当てている。欧州委員会は、多年度の領域情報及び情報伝達計画によって、これらの活動を支援する。東部 Stratcom タスクフォースは、構成国及び NATO との間においても、継続的に、共同活動を行う。虚偽情報の監視と並んで、ロシアの虚偽情報の影響に関し、東部 Stratcom タスクフォースは、東部パートナーシップ諸国及び構成国における周知活動を行った。東部 Stratcom タスクフォースは、虚偽情報に対する東部パートナーシップ諸国の Stratcom 能力の拡大及びその回復力のために、東部パートナーシップ諸国において、職員の訓練のステップアップも行った。NATO 事務総局及びリガとヘルシンキの研究拠点との間のより大きな協力は、東部パートナーシップ領域及びロシアからのジャーナリストの分析セミナー及び訓練セミナーの分担のような、将来を見据えている。

EU の新たな西バルカン戦略に従い、西バルカン諸国を標的とする虚偽情報活動に関して周知し、かつ、その活動に対処しつつ、この領域において、より実効的に、かつ、より多くの者に対し、EU の政策を伝えるため、西バルカン諸国に焦点を当てたタスクフォースが開始された。このタスクフォース及び欧州委員会は、ベストプラクティスに基づき、かつ、テーマ別のキャンペーン行動に焦点を当てて、この領域に向けたより戦略的で対象を絞った情報伝達及びメッセージ発信を狙いとする緊密な協力関係を構築した。しかしながら、特に国家機関を標的とする脅威の増大についての認識が欠けている。セキュリティ認識の文化を構築し、ハイブリッド脅威に対処するための国家機関の能力を増加させる必要性がある。

2017 年に設置された南部タスクフォースは、アラブ世界に対するアラビア語による伝達及び拡大を向上せさせるためのより精密なアプローチに向けた対テロリズムのプリズムのシフトを反映するため、その任務を調整した。Daesh または ISIS のみが過激主義の面における脅威ではないので、このタスクフォースは、広範な虚偽情報及び EU の曲解を削減するための仕事をする。この仕事は、欧州委員会と緊密に協力した上で、欧州連合のより大きな理解を構築するための欧州連合とその政策に関する肯定的な解説を策定すること、アラブ世界において欧州連合の活動に関するより戦略的な情報伝達を行うこと、そして、価値及び利益の共有を促進することにより、実施される。欧州委員会は、多年度の領域情報及び情報伝達計画によって、それらの活動を支援する。

行動 4：「ハイブリッドな脅威に対抗する」の研究拠点

2017 年に設置されたハイブリッド脅威への対抗の欧州研究拠点は、調査研究、訓練、教育及び演習を介して、ハイブリッド脅威に対抗するための参加国の個別の努力または集団的な努力を支援するための専門知識のハブとしての機能を提供している。この研究拠点は、EU 構成国及び NATO 加盟国の両者に対し、参加のために開かれている。近時、イタリア、オランダ、デンマーク及びチェコ共和国が参加国となり、合計で 16 か国となった。EU 及び NATO の両者は、運営委員会において、オブザーバーとして参加する。

2018 年、予算及び業務計画が合意された研究拠点は、その概念枠組みを構築し、3 つの関係コミュ

[4] 周知された時点で参照が挿入される。

ニティを創設した：すなわち、ハイブリッドな影響、脆弱性及び回復力、並びに、戦略及び防衛である。非国家参加者のサブグループが設置された。そのサブグループは、異なるテロリストグループ及びその代理者がどのように展開しているかを注視する。研究拠点は、多数のハイブリッド分析を公表し、また、ハイブリッドな脅威の共通理解を構築し、ベストプラクティスを共有し、そして、EU 及び NATO の共同体全域にわたる共通の対応を追求するための複数のハイレベル会合をホストした。

EU の対応の組織化：回復力の構築

回復力を構築することは、多数の政策分野における行動を要求する。それらの行動は、必ずしも脅威のハイブリッドな性質に特有のものではないが、それと共に実施されるものであり、より回復力のある EU がハイブリッド脅威への直面に対してより良く装備されていることを確保し得るものである。それゆえ、後述の各行動の下に行われた進捗状況の記述と関連する場合、特定の政策枠組み及び欧州連合によって実施された行動、とりわけ、安全の欧州連合に向けた仕事の一部として実施された行動への参照が行われる。それゆえ、この報告書は、同じ日に採択された実効的かつ真の安全の欧州連合をめざす月次進捗状況報告書と一緒に読まれなければならない[5]。

行動5：重要インフラの保護及び回復力

欧州委員会は、EU 内の重要インフラのための脆弱性指標及びハイブリッドな脅威に対する回復力のマニュアル案を策定した。このマニュアル案は、現在、構成国との協議を通じた確認の過程にある。マニュアルの最終版は、2018 年 11 月に採択される予定である。更に、脆弱性指標は、2018 年の NATO との同時統合演習（PACE18）の間に試されることになるが、個々の構成国からも関心が示された。重要インフラに対するハイブリッド攻撃の開始の早期の段階における早期の警告を容易なものとすることを狙いとする検知指標の更なる開発に注意が払われなければならない。ハイブリッドな脅威は、重要インフラの保護に関する欧州指令の来るべき評価においても検討されなければならない。更に、欧州委員会は、脆弱性の特定、早期検知及び指標、回復力、認識向上及び演習に特に焦点を絞って、ハイブリッドな脅威の多角的かつ横断的な特性に対応する科学的な支援を強化しているところである。

更に、欧州連合の重要な資産を保護するため、欧州委員会は、その投資が安全または公共の秩序を害するおそれがある場合において欧州連合への外国からの直接投資を審査するための枠組みを構築する規則の提案書を提出した[6]。この欧州委員会提案は、第三国の個人または事業者からの直接投資であって、就中、（電力、輸送、通信、データの記録保存、宇宙及びそれ以外の機微の施設を含め）重要インフラ、（人工知能、サイバーセキュリティ、軍事転用可能な技術を含め）重要技術、機微の情報へのアクセスを許容する重要な入力もしくは投資の供給の安全性またはそのような情報を管理する能力を害し得るものと関係するものである。

第 2 段階の一部としての、欧州防衛局の防衛及び安全保障部門における持続的な電力供給に関する協議フォーラム（CF SEDSS II）は、EU レベルの政策ガイド文書に翻訳される重要電力インフラ保護（PCEI）専門家グループによって準備される概念規定書の策定を更に支援するであろう。この文書は、

[5] COM(2018) 470 final.
[6] COM(2017) 487 final.

全ての国防関連重要電力インフラの防護及び回復力の強化における国防大臣のためのマネジメントのベストプラクティスを提案している。

行動6：EU の電力供給の安全性の増進及び原子力インフラの回復力の増進

2017 年 9 月に参加した後（共働通知「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」[7]）、欧州委員会は、サイバーセキュリティに関し、欧州電力情報共有及び分析センターを継続して支援している。

天然ガス供給の危機を防止するため、欧州委員会がリスクグループ内においてその実装と構成国間の協力を容易にしながら、構成国は、昨年採択された天然ガス供給のセキュリティ規則を実装しているところである。共通のリスク評価は、欧州委員会に対し、2018 年 10 月 1 日までに通知されなければならない。欧州委員会は、2019 年 3 月 1 日までに、予防行動計画及び危機管理計画を受け取ることであろう。構成国は、2018 年 12 月 1 日までに、2 国間連携協定を締結しなければならない。

電力リスクの準備における既存の法令上の格差に対応するため、目下交渉中のリスク対応準備規則は、リスクをどのように評価するか、一定の強制的な要素をもつリスク対応準備計画を準備すべき構成国の義務、危機状況をどのように取り扱うか、供給の安全性をどのように監視するかに関する規定を伴うものとなるであろう。リスク対応準備計画は、領域内の協力に関する手配、とりわけ、同時的な電力危機の状況をどのように管理するかに関する手配も含めなければならない。リスク対応準備規則の実装において、構成国は、この規則が発効した後、2 年以内に、最初の国内リスク対応準備計画を準備しなければならないであろう。その後、計画は、3 年毎にアップデートされなければならない。将来のリスク対応準備規則は、電力危機をシミュレートするため、構成国間において継続的かつ共同の演習を実施することも要求することになる。欧州委員会は、興味を示している構成国、共同調査センター及び電力調整グループとのそのような共同演習の準備を既に開始している。

原子力インフラの回復力に関し、構成国及び欧州委員会との情報交換、及び、それらの間における原子力の安全問題に関する情報交換は、短期間で改善されることになり、そして、追加的な取り組みのための分析が予定されている。原子力の安全規制の分析、封入された高放射性物質のより良い取扱いにおいて構成国を支援するためのガイドの可否に関する分析が遂行される。より長期的には、欧州委員会は、構成国が共通の利益をもつ場合、及び、情報交換及び共同活動についての合意された利益が存在する場合、原子力分野における活動を強化する予定である。欧州委員会は、核物質及び原子力施設の物理的防護に関する国際条約の EU 内における効果的な実装のための適切な措置も検討することになる。

防衛部門が関係する範囲内で、国防及び安全保障部門における持続的な電力供給のための協議フォーラムは、インフラの電力管理を向上させることにおいて国防部門を支援するため、「国防及び安全保障における持続的な電力管理のための行程表」を準備する。この協議フォーラムは、国防部門が、電力資源をより効率的になることを可能とするためにはいかにすべきかを研究し、国防部門による潜在的な研究に関するプロジェクトを産み出すための多数の技術（例：風力、太陽光、スマートグリッド、電力蓄積、バイオ燃料、バイオマス及び廃棄物の電力転換）の見直しを継続することであろう。

この文脈において、欧州防衛局の電力及び環境計画は、「家庭における」持続的な水道管理技術の

[7] COM(2017) 487 final.

介入の範囲を調査研究するための Smart Blue Water Camps 調査プロジェクトを通じて、及び、CSDP ミッションの費用及び軍事上の効率性を改善しつつ、電力問題、水問題及び廃棄物問題に対処するための軍事環境内における大規模なより広範な技術または電力及び環境技術の影向の実現可能性を調査研究する Smart Camps Technical Demonstrator 調査研究契約を通じて、その仕事を継続する。

行動7:輸送及び流通網の安全性

全ての輸送分野に関し、すなわち、民間航空、海運及び陸上輸送に関し、欧州委員会は、知識を獲得し、経験から学ぶため、ハイブリッドな性質をもつ先端的なセキュリティ上の脅威に関し、構成国、産業界及びそれら以外の利害関係者との間の集中討議をもつ。

EU の海事安全戦略行動計画の実装活動及び見直しの過程において、欧州委員会は、(海賊行為及び海事紛争を含め)運送及び貿易ルートを破壊し、EU の利益を害し得る海事上の安全性における傾向を分析しているところである。EU 構成国及び EEA 構成国が世界中の商船の 40%を管理しているという事実、及び、EU が重要な貿易圏であるという事実に鑑み、海事貿易ルートに対するハイブリッドな攻撃は、欧州の価値及び流通網に対して重大な破壊的影響をもち得る。海事部門におけるリスク分析及び先端脅威の分析は、それが適切なときは、特定の輸送立法をアップデートするための提案を導き得る。それは、共通情報共有環境(CISE)の開発の過程の下にあるものを含め、海事における認識の向上に関する継続的な仕事の基礎となるものでもあり、国内海事機関の間における IT 相互運用性を拡大するために構成国を支援することの提案を求める新たな要求は、近時、3 つの新たなプロジェクトを承認した(2018 年に開始)。

2016 年 9 月の国境及び沿岸警備パッケージ[8]の採択により、欧州議会及び理事会は、海事における状況認識を向上させるため、及び、一貫性があり、費用対効果のある支援を提供するため、相互に、及び、他の国内機関と共に、沿岸警備の職務を実施するそれらの機関の個々の任務の範囲内において、それらの機関の協力関係を強化するためにそれらの機関の職務を与える欧州国境沿岸警備局、欧州漁業監督局(EFCA)及び欧州海事安全局(EMSA)の基礎となる諸規則の中に、共通の条項[9]を盛り込んだ。この点に関し、沿岸警備の職務を遂行する機関の間のリスク評価の分野における相互運用性及び協力関係の拡大の共通点及び方法を指摘する研究結果[10]が 2017 年に公表された。

(港湾を含むがそれに限定されない)輸送関係の課題及び先端脅威は、航空機の安全に対するサイバー脅威、GPS ジャミング及びスプーフィング、通信衛星に対する脅威、または、高北緯及び北極における問題である。ヘルシンキのハイブリッド脅威への対抗のための研究拠点は、これらの輸送関連のハイブリッド脅威の分析にも貢献し、かつ、近時、港の防護に関する分析に着手した。EU の税関当局は、対外国境及び流通網の確保において重要な役割を維持しており、それによって、欧州連合の安全に貢献している。欧州委員会は、EU 内の税関が、必要な全ての情報を獲得し、構成国間におい

---

8 欧州の国境及び沿岸警備に関する規則(EU) 2016/1624

9 沿岸警備の職務:すなわち、(1)海事の安全及び船舶交通管理;(2)海難及び海事関係支援の職務;(3)漁業の監視及び監督;(4)海上国境管理;(5)海の環境保護;(6)人身取引及び密輸の防止及び抑止並びに関連する海法上の警察活動;(7)海上の捜索及び救助;(8)海上の監視及び臨検;(9)海上の税関の職務;(10)海上の事故及び災害への対応;並びに、(11)海事、船舶及び港湾の安全。

10 https://publications.europa.eu/en/publication-detail/-/publication/217db2fc-15d6-11e7-808e-01aa75ed71a1/language-en

てその情報をより効率的に共有し、共通のリスク法令及び構成国に特化したリスク法令を提供し、そして、リスクの高い荷送りをより効果的に絞ることを確保するため、高度貨物情報税関リスク管理システムを大きくアップグレードしているところである。EU の化学兵器、生物兵器、放射線兵器及び核兵器（CBRN）行動計画[11]の重要な優先事項の 1 つは、CBRN 物質の不正な持ち込みに対するより広い安全及び検知能力を確保することである。貨物情報システムの調整は、CBRN 物質が EU 内に不正に持ち込まれないようにするための国際的な流通網の監視及びリスクベースの管理を強化するために重要なことである。実効的かつ真に安全の欧州連合をめざす第 15 次進捗状況報告書は、CBRN リスクに対する準備を拡大するための EU の措置、並びに、とりわけ、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を拡大するための欧州委員会の行動計画の枠組み内において EU レベルで講じられる措置に関するより詳細な情報を提供している。

上級代表及び欧州委員会は、2018 年 3 月 28 日、欧州輸送ネットワークの軍民共用の可能性を開拓し、軍事輸送のための通関手続を簡素化し、そして、軍用の危険物の輸送のための法令上及び手続上の問題に対処するための行動計画を提出した。欧州委員会は、軍のモビリティの要件を調整するため、輸送インフラを支援するための欧州接続機能を介して実装される多年度財政枠組みの「防衛」クラスタに基づき、65 億ユーロの予算を提案した。その目的は、輸送インフラの軍民共用を可能とすることにある。

行動8：宇宙資産における回復力の構築

欧州連合の宇宙計画のための欧州委員会提案[12]は、Copernicus における政府衛星通信及び宇宙調査追跡支援枠組みを含め、セキュリティの側面を統合する。それは、Galileo 及び EGNOS のために既に設けられている措置に加え、ハイブリッドな脅威に対する回復力の側面をカバーするものである。

宇宙調査追跡[13]は、欧州及び国内の宇宙インフラ、設備及びサービスの長期の可用性を支援することを狙いとしている。それは、宇宙の物体の衝突、破壊及び制御不能な大気圏再突入を避けるための最初のサービスを 2016 年 7 月に開始した。宇宙調査追跡の国内運用センター及び EU 衛星センターは、宇宙状況認識データ基本政策のセキュリティの側面における理事会勧告[14]を考慮に入れたデータセキュリティの手段をもつ。

Galileo に関し、欧州委員会は、タイミング及び同期のための衛星ナビゲーションに依存する重要インフラが適正に機能するために重要なデータの提供のより良い保護を確保するための新たな手立てを講じつつある。電力網、電気通信ネットワーク及び金融市場のような、重要インフラにおけるサービスの提供のために Galileo が利用されていると考えられる。この文脈において、欧州委員会の外国からの直接の投資の審査のための枠組みを構築する規則案は、プロジェクトの例として、欧州グローバルナビゲーション衛星システム（GNSS）、Galileo 及び EGNOS、または、規則案の下にある外国からの直接投資の審査と関連をもち得る欧州連合の利益の計画を指示している[15]。

---

[11] COM(2017)610 final, 18.10.2017.
[12] COM(2018) 447 final, 6.6.2018.
[13] Decision No 541/2014/EU of European Parliament and Council of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support Framework
[14] Space Situational Awareness Data Policy (14698/12), 9.10.2012
[15] COM(2017)487 final の別紙参照。

EU の政府衛星通信イニシアティブは、欧州連合及び構成国の任務、運営及び重要インフラに対し、衛星通信への保証のある安全なアクセスを提供することであろう。これは、宇宙、輸送及び電力インフラを含め、広範なインフラに対するハイブリッドな脅威に対抗するための重要なツールの 1 つである。

行動9：防衛能力の調整及びEU の能力の開発

2017 年 6 月 7 日に開始した欧州防衛基金は、戦略上の検討課題に対して効果的に対応するために欧州内の防衛上の共同活動を増加及び維持するための構成国の努力にインセンティブを与えるための大きな歩みを進めた。基金の能力の視野の範囲内において、EU は、とりわけ、共同の防衛発展プロジェクトのための国内予算を補完する。その目的のために、欧州委員会は、2019 年～2020 年のために 5 億ユーロの予算をもつ欧州防衛産業開発計画を定める規則を 2017 年 6 月に提案した。欧州議会及び理事会は、2018 年 5 月 22 日、規則案の暫定合意に達した。EU の次期の多年度財政枠組みに関し、欧州委員会は、共同防衛能力開発プロジェクトのための 89 億ユーロを超える予算を予定し、130 億ユーロの意欲的な予算をもつ統合欧州防衛基金を提案した。能力開発におけるハイブリッドな脅威への対抗の影響の可能性は、2018 年 6 月に構成国間で合意される改訂能力開発計画の中に統合されることになるであろう。

行動10：保健衛生上の準備及び調整の仕組み

保健衛生上の準備は、CBRN リスクに対する準備全部の中でも非常に重要な構成要素の 1 つである。このことが、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を拡大するための欧州委員会の行動計画に基づき、欧州委員会が手立てを講ずる理由であり、とりわけ、専門知識を効果的に共有するための取り組みに対する努力が尽くされてきた。

それゆえ、欧州委員会は、国境を越える重大な脅威に対する準備及び対応計画を試すための越える EU 及び第三国を通じた保健衛生部門、市民保護部門及び安全保障部門のための演習である Chimera を設けた。この演習の想定シナリオは、ハイブリッドな脅威に対する対応における国内レベル及び EU レベルの既存の仕組み、システム及び通信手段を試すため、病院を含め、重要インフラに対するサーバー攻撃と組み合わされた伝染病原因菌の意図的な散布を含めていた。演習は、ルクセンブルクにおいて、2018 年 1 月 30 日～31 日に行われた。EU レベル及び国内レベルの保健衛生部門、市民保護部門及び安全保障部門の相互運用性及び調整の国境を越える能力構築及び向上、並びに、国際的な関係者との共働活動を支援に貢献した。演習は、ハイブリッドな脅威の危機管理における全ての利害関係者の現在の責任及び役割を定めることを助けることともなった。早期警戒対応システム（EWRS）、欧州委員会の国境を越える警戒システム（ARGUS）、共通緊急通信情報システム（CECIS）及び理事会統合政策危機対応措置（IPCR）は、それらがどのように相互作用するかに関し、試された。実効的かつ真の安全の欧州連合第 15 次報告書は、CBRN リスクに対する準備を拡大するための EU の措置の更に詳細な情報を提供している。

2018 年 4 月、欧州委員会は、2018 年末よりも前の採択を求めることを狙いとするワクチン予防可能疾患に対する EU の共同活動を強化するための理事会勧告を求める通知及び提案書を公表した。それは、ワクチン接種の躊躇との取り組み、ワクチン接種計画の持続性の拡大、及び、ワクチンの調査研

究と開発の実効性の強化を狙いとしている。

欧州医療団体の観点から、ノルウェー緊急医療チームは、世界保健機関（WHO）によって、ミニマムの品質基準を遵守するものと区分された。2018 年 4 月、WHO 欧州地域緊急医療チームの最初の地域会合が開催された;この会合は、欧州委員会、世界保健機関及び地域グループ議長としてのベルギーの保健機関によって共同主催された。

大規模熱傷原因疾病の管理のための仕組みを開発するため、現在、欧州熱傷学会議及び構成国が緊密に共働する準備が進行中である。2018 年 10 月早々、欧州委員会及び構成国は、その仕事をしめくくるためのワークショップにおいて会合する。

行動11 :CSIRT（サイバーセキュリティインシデント対応チーム）ネットワーク及びCERT-EU とNIS 指令

CERT-EU は、定期的に及び不定期に、重要部門と関連するサイバー脅威評価の成果物を公表する。異なる輸送モード（航空運送、海上運送及び陸上輸送）に関し、欧州委員会は、継続的に監視を行い、また、部門別の取り組みがネットワーク及び情報システムの安全性に関する指令（NIS 指令）の適用のある部門横断的な能力と一貫性をもつことを確保する。

2017 年 9 月、欧州防衛局及び EU の理事会のエストニア大統領職は、政治レベルのサイバーセキュリティインシデントの調整活動及び攻撃的なサイバーキャンペーンの政治的影響の認識を向上させるため、CYBRID17 と命名された EU の防衛大臣のための戦略的机上サイバー演習を実施した。その演習は、状況認識、危機対応の仕組み及び戦略通信に焦点を当てた。欧州防衛局は、この演習の要素を、2018 年 9 月までに設立される欧州セキュリティ及び防衛コレゲートの教育、訓練、評価及び演習プラットフォームの中に移植する。EU の大統領職による同様のハイレベル演習の将来の実施が検討中である。

行動12 : サイバーセキュリティに関する契約による官民パートナーシップ

欧州委員会は、欧州におけるデジタルセキュリティ及びプライバシー産業の競争力及び技術革新能力を刺激するため、欧州サイバーセキュリティ機関（ECSO）との間で、サイバーセキュリティに関する官民パートナーシップに署名した。EU は、利用者及び産業界をサイバー攻撃から防護するため、このパートナーシップにおいて、4 億 5000 万ユーロに上る投資を行う。cPPP は、2020 年までに、18 億ユーロの投資の契機となることを期待している。

サイバーセキュリティに関し、回復力、抑止力及び防衛に関する共同通知:EU のための強力なサイバーセキュリティの構築[16]は、同共同通知に定める EU のサイバーセキュリティの組織構造及び能力に対して大きな加速を提供するための措置を定めた。しかしながら、EU におけるサイバーセキュリティは、不十分な投資と調整によって妨げられている。EU は、共同通知の中に定めるサイバーセキュリティに対応することを求め続けている。

[16] JOIN (2017) 450 final

行動13：電力部門の回復力

2018 年 6 月、欧州委員会は、特に電力部門に対応するため、及び、同部門のためのネットワーク及び情報システムの安全性に関する指令（NIS 指令）の実装に関する構成国向けのガイドを提供するため、NIS 協力グループの下に電力部門のワークストリームを設ける。それと並行して、欧州委員会は、電力部門におけるサイバーセキュリティのグッドプラクティスを見出すため、及び、NIS 指令の適用のない事業者に対処するため、NIS 指令の適用範囲を超える特定のサイバーセキュリティのガイドに関し、作業する。欧州委員会は、認識を向上させるため、グッドプラクティスを共有するため、（送電システム事業者と配電システム事業者との間の国境を越える）協力を拡大するため、物的な措置、新たなリスク並びに教育及び技能に対処するため、電力部門におけるサイバーセキュリティ上の問題と関連する出来事の情報共有の取り組みを継続する。

長期的には、欧州委員会は、近時、立法手続に乗せられた電力規則改正案[17]の中で提案したように、サイバーセキュリティ部門に特化した法令に関するネットワークコードを構築する。

行動14：金融部門の回復力：情報共有プラットフォーム及びネットワーク

欧州委員会の Fintech 行動計画は、金融市場参加者の間におけるサイバー脅威の情報共有を制限する潜在的な障壁に対処し、それらの障壁を解消するための解決策の可能性を示すものである。CERT-EU は、インシデントに関する情報共有において、より大きな役割を演ずる。

行動15：輸送部門におけるサイバー攻撃に対する回復力

サイバーセキュリティ攻撃から輸送部門を防護することは、欧州委員会にとって、高い優先度をもつ。民間航空において、サイバーセキュリティの観点からの良好な進捗があるが、欧州の半分に影響を与えた近時の EUROCONTROL における IT インシデントが示したように、技術的な問題またはサイバーセキュリティ上の脅威から生ずるシステムの脆弱性は、これを捨て去ることが許されない。欧州委員会は、この輸送分野において、欧州航空安全局と緊密に協力する。CERT-EU は、サイバー脅威の取扱いに関してこれらの組織及びその利害関係者を助けるため、EUROCONTROL との間でサービスレベル合意に署名し、また、欧州航空安全局との間で協力覚書に署名した。

海上輸送においては、海運業界は、サイバーセキュリティ運用指針を発行し、その後、主としてグローバルな観点及びアプローチにおいて、国際海事機関において審議し、これを採択した。欧州の港湾及び港湾設備におけるサイバーセキュリティは、政策上の高い優先度を維持しており、ネットワーク情報セキュリティ指令の実装及びフォローアップの過程において、構成国、産業界及び利害関係者との間で検討され、継続的に意見交換が行われている。

欧州委員会は、輸送部門のセキュリティ管理者及び専門家がサイバーセキュリティ上のリスクをより良く特定し、評価し、そして、削減することを支援するため、推奨されるグッドプラクティスを伴う全体的かつ相互的なサイバーセキュリティ情報ツールキットを開発する予定である。

[17] Proposal for a Regulation of the European Parliament and of the Council on the internal market for electricity (recast) - COM/2016/0861 final

行動16：テロリスト資金提供への対抗措置

昨年、欧州委員会は、安全の欧州連合定期報告書の中で報告されているとおり、テロリスト資金提供に対抗するための大きな仕事を行った。最も近いところでは、2018 年 4 月のセキュリティパッケージ[18]の中において、欧州委員会は、重大犯罪及びテロリズムとの闘いについて職責を負う機関の間の協力をステップアップするため、及び、重大犯罪行為の防止、検知、捜査または訴追に関する資金情報及びそれ以外の情報の利用を容易にする指令の提案[19]と共に、資金情報へのそれらの機関のアクセス及び利用を拡大するための更なる措置を講じた。テロリスト資金提供に対抗するために EU のレベルで実施された最近の仕事の更に詳細な情報は、実効的かつ真の安全の欧州連合をめざす第 15 次進捗状況報告書の中にある。

資金洗浄犯罪行為に対する制裁を整合化するため、欧州委員会は、2018 年中旬に採択されることを予定する立法を提案した。更に、高リスク第三国の検査の拡大、仮想通貨交換プラットフォームの検査、前払式決済手段に適用される透明性措置、金融情報ユニットの新たな権限、及び、集中登録簿または金融情報ユニットのための電子的なデータ検索システムを介する銀行口座及び決済口座の保有者に関する情報への迅速なアクセスのような多数の措置を強化するため、第 5 次資金洗浄禁止指令が本年 5 月に採択された。

行動17：過激化を防止する行動及び違法なコンテントの除去に関する手続の強化の必要性の分析

オフライン及びオンラインの暴力的な過激化の防止は、昨年における欧州委員会の優先事項であった。EU レベルの仕事をステップアップするため、欧州委員会は、EU の防止政策の調整、範囲及び影響に関する勧告を提供するための過激化に関するハイレベル専門家グループを設置した。ハイレベル専門家グループは、2018 年 5 月 18 日、その最終報告書を提出した。その報告書は、EU の調整の仕組みの構築を求める勧告を含んでいる。

オンラインの違法コンテントに関し、欧州委員会の 2018 年 3 月 1 日の勧告の採択の後、そのようなオンラインのコンテントへのアクセシビリティの削減に関心の重点が移動しつつある。欧州委員会は、既存の法的枠組みを補完するための立法措置の可否を含め、オンラインの違法コンテントの迅速かつ積極的な検知及び削除を確保するため、現在の努力が十分なものであるか否か、または、追加的な措置が必要であるか否かを判断するための影響評価を開始した。この分野において実施された欧州委員会の仕事の更に詳細な情報は、実効的かつ真の安全の欧州連合をめざす第 15 次進捗状況報告書の中にある。

Facebook、Twitter、Google（YouTube）及び Microsoft によるオンラインの違法なヘイトスピーチに対抗するための行動準則は、迅速かつ積極的な効果をあげている。行動準則は、それらの会社が連絡を受けた違法なヘイトスピーチと思われるものを迅速に検討し、削除することに関し、これらの会社は、大きな進展を果たした。2018 年 1 月に発行された行動準則の実装に関する欧州委員会の第 3 次監視演習は、行動準則によって想定されていたとおり、ヘイトスピーチコンテントの平均 70％が削除され、24 時間以内にヘイトスピーチの検討が行われたという結果を示した。この行動準則は、産業界におけ

[18] COM(2018) 211 final.
[19] COM(2018) 213 final.

る標準となり、近時の Instagram 及び Google+の行動準則への加入の決定を推進している。2018 年 3 月、欧州委員会は、自動検出、透明性及び利用者に対するフィードバック、並びに、言論の自由を保護するための標準のような、オンラインプラットフォームに対する追加措置も提案した[20]。

過激化及びオンラインのヘイトスピーチに対して既に執られた行動を越えて、選挙に対するサイバー可能化脅威を防止し、削減するための手立てが講じられなければならない。

行動18：近隣諸国及び第三国との協力の拡大

欧州連合は、就中、改訂された欧州近隣国政策のセキュリティの面を発展させることにより、パートナー諸国のセキュリティ部門における能力及び回復力の構築にその焦点を集中させた。ハイブリッドな脅威に対抗するためのパートナーの能力を拡大するという目的のために、その目的専用のハイブリッドリスク調査は、パートナー諸国の脆弱性を特定しつつあり、的を絞った支援を提供している。EEAS は、欧州委員会と共同して、モルドバ共和国の調査を実施した。2018 年、ヨルダン及びジョージアは、EU に対し、公式に、それらの国の個別の需要に対応した質問事項の作成という脆弱性調査の最初の段階を実施することを要請した。ウクライナにおいて、技術支援使節を介して、とりわけ重要インフラのために構築されるサイバーセキュリティ能力に関する補完的な作業が実施された。その間、欧州委員会は、2018 年早々、特にアフリカ及びアジアの第三国諸国のサイバー回復力を拡大することを意図する新たな包括的な計画も開始した。

EU は、国境監視作業グループ内において、国際原子力機関及び合衆国政府との間で原子力の安全性の能力構築の案及び計画に関する意見交換を継続している。欧州原子力安全性訓練センター（EUSECTRA）は、原子力の安全性における防止及び権利に関する訓練、並びに、原子力インシデントモジュールへの対応を提供する。化学兵器のリスク、生物兵器のリスク、放射線兵器のリスク及び核の安全性上のリスクに対する準備を拡大するための欧州委員会の行動計画は、対テロリズム及び関連第三国との安全保障対話を含め、重要な国際的なパートナーとの間の協力に関する特別の行動をもっている。

ほぼ全部の近隣パートナー諸国が含まれている EU の基金による情報イニシアティブの CBRN センター[21]は、「ハードセキュリティ」構造を内包する脅威を含め、これらの脅威に対する防止、準備及び対応におけるパートナー諸国の国内及び地域の能力の増強に関する仕事を継続する。

東部近隣諸国地域及び南部近隣諸国地域において、自然災害及び人為的災害に対する防止、準備及び対応（PPRD）の地域計画に基づき、市民保護の訓練及び演習が計画されている。PPRD 南部地域の第 3 段階は、2018 年に開始し、その間、2018 年 11 月に PPRD 東部の第 2 段階終了するが、延長される可能性がある。CBRN 地域情報センター並びに PPRD 南部計画及び PPRD 東部計画との緊密な連携が確保される。

危機の防止、対応及び復旧

国内レベル及び EU レベルにおける長期的政策を通じてハイブリッドな脅威により生じた結果を削

[20] COM(2018) 1177 final

[21] ラバト、アルジェ、アンマン及びトビリシの地域 CBRN センターと共に。

減することは可能であるが、迅速かつ調整された態様でハイブリッドな脅威を防止し、それに対応し、そこから回復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、依然として重要である。ハイブリッドな脅威を引き金として発生する出来事への迅速な対応は、重要である。昨年、この分野において、ハイブリッド攻撃の際の危機管理プロセスを定める EU における現在の業務遂行手順により、大きな進展が達成された。継続的な監視及び演習が推進される。

行動 19:複合ハイブリッド脅威への対応における戦略的意思決定能力を向上させるための共通の業務遂行手順及び演習

EU 業務遂行手順は、2016 年 6 月の共同スタッフ作業文書によって定められた。この手順は、汎機関の危機対応のための盤石なガイドを提供する。EUPACE17 の間、この手順は、ハイブリッドシナリオに対して試され、機関相互のやりとりを容易にするための非常に貴重なツールであることを証明した。更に、この手順は、様々なレベルの対応、すなわち、潜在的な戦略レベル、運用レベル及び技術レベルの間、並びに、(対外危機に関する)EU の 3 つの主要な対応、ARGUS(情報共通のための欧州委員会の域内 IT ベースプラットフォーム)及び理事会の統合政治危機対応プラットフォームの間における相互関係の接点を定めた。この手順は、CMX'17 の際の NATO との間の同時演習の間においても、その価値を証明した。PACE18 における次の一連の演習は、2018 年 11 月に実施され、指定された将来の練習を考慮に入れた上で、手順のアップデートが検討されることになる。

2017 年 9 月及び 10 月、EU は、NATO との間で、大規模なハイブリッド危機の場合における 2 つの組織の間の準備及び相互関係を試す最初の同時統合演習(PACE17)を実施した。準備のフェーズにおいては、ハイブリッド作戦書の 4 つの分野:すなわち、早期警戒/状況認識;戦略通信;サイバー防衛;危機防止及び危機管理の全部について、緊密なスタッフ交換が実施された。EUPACE17 の間における EU と NATO との間の相互関係の規模は、前例のないものである。それは、大統領職が主宰する統合政治危機対応ラウンドテーブルに NATO が参加し、EU の上級官吏が北大西洋理事会の討議に参加する最初の機会でもあった。練習・学習のプロセスは、EU と NATO との間の危機対応の仕組みの相互関係、並びに、安全な通信の必要性、特に、将来において、発信者の管理の必要性を全面的に尊重し、迅速かつ安全な交換を確保することを狙いとする通信の必要を含め、2 つの組織の官吏の間における機密情報の交換と関連する検討課題を含む複数の側面に焦点が当てられた。

EU が主導的な組織となる 2018 年の同時統合演習は、進行中である。

行動20:広範囲の重大なハイブリッド攻撃発生の場合における TFEU 第222 条及び TEU 第42 条第7 項の適用可能性及び実務上の実装の検討

EU の連携条項及びその支援の仕組み、並びに、相互の交流及び第 5 条の集団的防衛を含む NATO との間の対応の仕組みの適用可能性は、更に討議が重ねられ、ハイブリッド演習シナリオの中で試されることになる。ハイブリッド脅威への対抗のためのヘルシンキ研究拠点は、調査研究及び演習の両面に関心を示し、作業を実施する準備を整えており、構成国と同盟国との間の理解の共有の発展を助ける。

行動 21：共通安全保障防衛政策の中でハイブリッドな脅威に対抗する軍事行動の統合、開発及び調整

共通対外安全保障政策／共通安全保障防衛政策を支持する統合された軍事能力の職務、並びに、その後の 2016 年 12 月の軍事専門家のセミナー、及び、2017 年 5 月の欧州連合軍事委員会作業グループのガイドに対応して、2017 年 7 月に「共通安全保障及び防衛政策の中におけるハイブリッドな脅威への対抗に対する EU の軍事的貢献」に関する軍事助言が完了した。この仕事は、概念開発実装計画を介して更に進められている。ハイブリッド脅威への対抗のための欧州研究拠点と協議した上で、欧州連合軍事参謀部は、共通安全保障及び防衛政策の任務及び作戦を介する場合を含め、軍がどのようにしてハイブリッドな脅威への対抗に貢献し得るかに関する概念を開発中である。

加えて、EU 軍事参謀部と構成国は、日々、EU Hybrid Fusion Cell に対して軍事情報上の支援を提供することにより、早期警戒の拡張を可能とし続けている。単一情報分析部は、EU 及び個々の構成国を標的とする虚偽情報キャンペーンへの対抗を助ける軍事上の助言に貢献することにより、EEAS の Stratcom タスクフォースを支援する。

ハイブリッドな脅威に対抗するための軍事能力は、NATO との間の 2018 年同時統合演習（PACE18）の間に試されることになる。PACE18 のハイブリッドシナリオに基づき、EU 軍事参謀部及び NATO 国際軍事参謀部は、義務が重複している場合、吸収の原則に基づき、それぞれの組織の意思決定の自律性とデータ保護法令を尊重しつつ、ハイブリッドな脅威への対抗における補完性を確保するための EU と NATO 間のシナリオベースの非公式な意見交換をもつ。

EU と NATO 間の協力

行動 22：状況認識、戦略通信、サイバーセキュリティ及び「危機防止及び危機管理」に関する EU と NATO 間の協力

ハイブリッドな脅威への対抗は、EU と NATO 間の相互関係の重要分野の 1 つであり続けている。それは、ハイブリッド脅威が発生した場合において、2 つの組織が移動可能な資源及び能力が補完的なものであること、並びに、そのような脅威の防止、検知及び対応のための構成国及び同盟国の能力を拡大することの現実化することを基礎としている。PACE17 演習は、2 つの組織の「作戦書」を試し、そして、それを通じて、被害を受けた国を迅速かつ実効的に支援する仕事のためのそれらの組織の能力を試した。得られた経験に照らし、2 つの「作戦書」は、改訂され、アップデートされることになる。戦略通信の分野においては、ウクライナ、ボスニア・ヘルツェゴビナ、モルドバ共和国及びジョージアを支援するための協議が実施された。

2017 年 9 月、関連する活動に関する情報交換のため、及び、とりわけ、重要インフラ保護の分野における今後の作業の提案を行うため、重要戦略部門の専門家と共に、EU と NATO 間の回復力ワークショップが開催された。

2018 年において、Military Mobility は、軍の資材及び要員の移動を容易にするためのプロジェクトの 1 つであり、それは、構成国と同盟国の対応時間を遅延させることを特に狙ったハイブリッド脅威によって示されるような検討課題を考慮に入れることができるーそれは、将来の同時演習のための分野

の 1 つであり、一連の EUPACE19～EUPACE 20 の中で検討される。

サイバー訓練の努力の調整は、より緊密な相互関係にとって重要な分野の 1 つである。NATO は、2016 年 6 月の ENISA の CyberEurope 机上演習にもオブザーバーとして参加した。

結 論

様々な発生源からの進化するハイブリッド脅威の状況認識の向上及び回復力の構築は、なお検討課題であり続けており、EU の継続的な努力を必要とする。

共同枠組みは、情報の共有と交換の交換から、重要インフラの保護とサイバーセキュリティの強化、過激化と暴力的な過激主義からの社会の回復力の構築まで、非常に幅広いセットの行動をもっている。ハイブリッド脅威への対抗のための EU の枠組みは、危険な攻撃のストレスに耐え、それに対して調整された態様で対応し、そして、最終的に回復するための EU と構成国の能力を強化することを狙いとする様座な措置を通じて、構成国に対して支援を与えることを可能とした。

ハイブリッド脅威への EU の対応は、また、多数の演習の中で、NATO と共同して試され、演習を受けてきた。EU と NATO 内の多数の関係者の間の緊密な協力は、回復力構築の努力の鍵である。加えて、近隣パートナー諸国の脆弱性の特定及びハイブリッド脅威に対抗する能力構築の強化においてそれらの国々を支援することは、対外的な脅威の本質の理解を向上させることに資するものであり、それによって、EU 近隣諸国の安全保障の拡大をもたらすものである。