RECOMMANDATIONS

RECOMMANDATION (UE) 2017/1584 DE LA COMMISSION

du 13 septembre 2017

sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 292,

considérant ce qui suit:

(1) Le recours aux technologies de l'information et de la communication et la dépendance à l'égard de ces technologies sont désormais des aspects fondamentaux dans tous les secteurs d'activité économique, eu égard à l'interconnexion et à l'interdépendance sans précédent de nos entreprises et de nos citoyens par-delà les secteurs et les frontières. La survenance d'un incident lié à la cybersécurité touchant des organismes implantés dans plusieurs États membres, voire dans toute l'Union, et risquant de perturber gravement le marché intérieur et, plus généralement, les réseaux et les systèmes d'information sur lesquels reposent l'économie, la démocratie et la société dans l'Union est un scénario auquel les États membres et les institutions de l'Union européenne doivent être bien préparés.

(2) Un tel incident peut se muer en crise à l'échelle de l'Union lorsque les perturbations qu'il provoque dépassent les capacités d'action du seul État membre concerné ou lorsqu'il frappe plusieurs État membres en s'accompagnant de répercussions techniques et politiques si vastes qu'il requiert une coordination et une réaction rapides à l'échelle politique dans l'Union.

(3) Étant donné que les incidents de cybersécurité peuvent déclencher une crise plus large et toucher des secteurs d'activité autres que les seuls réseaux et systèmes d'information et de communication, la réaction qui s'impose, quelle qu'elle soit, doit comprendre des mesures d'atténuation tant intérieures qu'extérieures au cyberespace.

(4) Les incidents liés à la cybersécurité sont imprévisibles et surviennent et évoluent souvent dans des délais très courts, de sorte que leurs victimes et les entités chargées d'y répondre et d'en atténuer les effets doivent coordonner rapidement leur réaction. De plus, les incidents liés à la cybersécurité ne se limitent pas à une zone géographique déterminée et peuvent survenir simultanément ou se répandre instantanément dans un grand nombre de pays.

(5) L'efficacité de la réaction aux incidents et crises de cybersécurité majeurs à l'échelle de l'Union européenne suppose une coopération rapide et efficace entre toutes les parties concernées et dépend de l'état de préparation et des capacités des divers États membres, auxquels s'ajoute une action conjointe et coordonnée s'appuyant sur les capacités de l'Union. La rapidité et l'efficacité des réactions aux incidents sont donc tributaires de l'existence de procédures et de mécanismes de coopération préalablement établis et, dans la mesure du possible, bien éprouvés, dans le cadre desquels des responsabilités et des rôles précis sont assignés aux principaux acteurs aux niveaux national et européen.

(6) Dans ses conclusions ([1]) du 27 mai 2011 sur la protection des infrastructures d'information critiques, le Conseil a invité les États membres de l'Union à «renforcer la collaboration entre les États membres et contribuer, en s'appuyant sur l'expérience acquise et les résultats obtenus au niveau national en matière de gestion de crise et en coopération avec l'ENISA, à la mise au point de mécanismes de coopération européens en cas d'incident informatique, qui devront être mis à l'épreuve dans le cadre du prochain exercice "CyberEurope" en 2012».

(7) La communication de 2016 intitulée «Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité» ([2]) encourageait les États membres à tirer le meilleur parti possible des mécanismes de coopération prévus par la directive SRI ([3]) et à renforcer la

([1]) Conclusions du Conseil sur la protection des infrastructures d'information critiques «Réalisations et prochaines étapes: vers une cybersécurité mondiale», document 10299/11, Bruxelles, le 27 mai 2011.
([2]) COM(2016) 410 final du 5 juillet 2016.
([3]) Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

coopération transfrontalière en matière de préparation à un cyberincident de grande ampleur. Elle précisait, en outre, qu'une approche coordonnée de la coopération en cas de crise entre les différents éléments du cyberécosystème, qui serait définie dans un «plan d'action», améliorerait la préparation et que ce plan d'action devrait également garantir des synergies et une cohérence avec les mécanismes existants de gestion des crises.

(8) Dans les conclusions du Conseil ([1]) relatives à la communication précitée, les États membres ont appelé la Commission à proposer un plan aux organes prévus par la directive SRI et aux autres parties prenantes. Or la directive SRI ne prévoit pas de cadre de coopération à l'échelle de l'Union pour parer aux incidents et crises de cybersécurité majeurs.

(9) La Commission a procédé à des consultations avec les États membres à l'occasion de deux ateliers distincts qui ont eu lieu les 5 avril et 4 juillet 2017, en présence de représentants des centres de réponse aux incidents de sécurité informatique (CSIRT) des États membres, du groupe de coopération institué par la directive SRI et du groupe horizontal «Questions liées au cyberespace» du Conseil, ainsi que de représentants du Service européen pour l'action extérieure (SEAE), de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), d'Europol/EC3 et du secrétariat général du Conseil (SGC).

(10) Le plan d'action pour une réaction coordonnée aux incidents et crises de cybersécurité majeurs au niveau de l'Union, annexé à la présente recommandation, est la résultante des consultations évoquées ci-dessus et complète la communication «Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité».

(11) Il énonce et décrit les objectifs et les modalités de la coopération entre les États membres et les institutions, organes, bureaux et agences de l'Union européenne (ci-après les «institutions de l'Union européenne») dans les réactions aux incidents et aux crises de cybersécurité majeurs et explique comment les mécanismes de gestion de crise existants peuvent exploiter pleinement les structures existantes en matière de cybersécurité à l'échelle de l'Union européenne.

(12) Dans un scénario de crise de cybersécurité au sens du considérant 2, la coordination de la réaction de l'Union au niveau politique s'effectuera au sein du Conseil en recourant au dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR) ([2]), tandis que la Commission fera appel au processus transsectoriel de haut niveau ARGUS ([3]) pour la coordination en cas de crise. Si la crise comporte d'importantes implications liées à la politique extérieure ou à la politique de sécurité et de défense commune (PSDC), le système de réponse aux crises (SRC) ([3]) du Service européen pour l'action extérieure (SEAE) sera activé.

(13) Dans certains domaines, des mécanismes sectoriels de gestion des crises à l'échelon de l'Union européenne prévoient une coopération en cas d'incident ou de crise de cybersécurité. Ainsi, dans le cadre du système mondial de navigation par satellite (GNSS) européen, la décision 2014/496/PESC du Conseil ([4]) définit déjà les rôles respectifs du Conseil, du haut représentant, de la Commission, de l'Agence du GNSS européen et des États membres dans le cadre de la chaîne de responsabilités opérationnelles mise en place afin de réagir à la menace pesant sur l'Union, sur les États membres et sur le GNSS, y compris en cas de cyberattaque. Il convient, dès lors, que la présente recommandation respecte ces mécanismes.

(14) C'est aux États membres qu'il appartient au premier chef de répondre aux incidents et crises de cybersécurité majeurs qui les touchent. Un rôle important est néanmoins dévolu à la Commission, au haut représentant et aux autres institutions ou services de l'Union européenne, qui découle du droit de l'Union ou du fait que les incidents et les crises liés à la cybersécurité peuvent avoir une incidence sur tous les pans de l'activité économique au sein du marché unique, sur la sécurité et les relations internationales de l'Union ainsi que sur les institutions elles-mêmes.

(15) Au niveau de l'Union, les acteurs clés qui interviennent dans les réactions aux crises comprennent les structures et mécanismes nouvellement créés en vertu de la directive SRI, à savoir le réseau des centres de réponse aux incidents de sécurité informatique (CSIRT), ainsi que les agences et organismes concernés, à savoir l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), le Centre européen de lutte contre la cybercriminalité au sein d'Europol (Europol/EC3), le Centre d'analyse du renseignement de l'Union européenne (INTCEN), la direction «Renseignement» de l'État-major de l'Union européenne (EUMS INT) et la salle de veille (SITROOM) coopérant dans le cadre de la SIAC (capacité unique d'analyse du renseignement), la cellule de fusion de l'Union européenne contre les menaces hybrides (au sein de l'INTCEN), l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne (CERT-UE) et le Centre de coordination de la réaction d'urgence de la Commission européenne.

(16) La coopération entre les États membres pour répondre aux incidents de cybersécurité au niveau technique est assurée par le réseau des CSIRT institué par la directive SRI. L'ENISA assure le secrétariat du réseau et appuie

([1]) Document 14540/16, 15 novembre 2016.
([2]) Pour plus d'informations, voir le point 3.1 de l'appendice «Gestion des crises, mécanismes de coopération et acteurs au niveau de l'Union européenne».
([3]) Ibid.
([4]) Décision 2014/496/PESC du Conseil du 22 juillet 2014 sur les aspects du déploiement, de l'exploitation et de l'utilisation du système mondial de navigation par satellite européen portant atteinte à la sécurité de l'Union européenne et abrogeant l'action commune 2004/552/PESC (JO L 219 du 25.7.2014, p. 53).

activement la coopération entre les CSIRT. Les CSIRT nationaux et la CERT-UE coopèrent et échangent des informations sur une base volontaire, y compris, le cas échéant, pour répondre à des incidents de sécurité qui touchent un ou plusieurs États membres. À la demande du représentant du CSIRT d'un État membre, ils peuvent discuter et, si possible, identifier une réponse coordonnée à un incident identifié qui relève de la juridiction de ce même État membre. Les procédures applicables seront définies dans les procédures opératoires standards (POS) ([1]) du réseau des CSIRT.

(17) Le réseau des CSIRT est également chargé de débattre, d'étudier et d'identifier d'autres formes de coopération opérationnelle, notamment en rapport avec les catégories de risques et d'incidents, les alertes précoces, l'assistance mutuelle, les principes et modalités d'une coordination lorsque les États membres réagissent à des risques et incidents transfrontaliers.

(18) Le groupe de coopération institué par l'article 11 de la directive SRI est chargé de fournir des orientations stratégiques pour les activités du réseau des CSIRT, de discuter des capacités et de l'état de préparation des États membres et, à titre volontaire, d'évaluer les stratégies nationales en matière de sécurité des réseaux et des systèmes d'information et l'efficacité des CSIRT, ainsi que d'identifier les bonnes pratiques.

(19) Un volet spécifique des travaux du groupe de coopération consiste actuellement à élaborer des lignes directrices en matière de notification d'incidents, conformément à l'article 14, paragraphe 7, de la directive SRI, relatives aux circonstances dans lesquelles les opérateurs de services essentiels sont tenus de notifier les incidents en vertu de l'article 14, paragraphe 3, ainsi que la forme et les modalités de ces notifications ([2]).

(20) Pour pouvoir opérer des choix éclairés, il est indispensable d'acquérir, par des rapports, des évaluations, des recherches, des enquêtes et des analyses, une connaissance et une compréhension de la situation en temps réel, de l'état des capacités de réaction aux risques et des menaces. L'appréciation de la situation et ce, par toutes les parties concernées, est essentielle pour permettre une réaction coordonnée efficace. Cette appréciation de la situation intègre des éléments relatifs aux causes ainsi qu'aux conséquences et à l'origine de l'incident. Il est admis qu'elle dépend de l'échange et du partage d'informations entre les parties concernées effectués dans un format approprié, selon une taxonomie commune pour décrire l'incident et d'une manière suffisamment sécurisée.

(21) Les réactions aux incidents de cybersécurité peuvent prendre de nombreuses formes, comprenant la recherche de mesures techniques pouvant nécessiter la collaboration de plusieurs entités pour enquêter sur les causes techniques de l'incident (par exemple analyse de logiciels malveillants) ou la recherche de moyens permettant aux organisations de vérifier si elles ont été touchées (par exemple indicateurs de compromis), mais aussi des décisions pratiques sur l'application de ces mesures et, à l'échelon politique, la décision de recourir ou non à d'autres instruments, comme le cadre pour une réponse conjointe face aux actes de cybermalveillance ([3]) ou le protocole opérationnel de l'Union européenne de lutte contre les menaces hybrides ([4]), selon l'incident.

(22) La confiance des entreprises et des citoyens européens dans les services numériques est essentielle à la prospérité du marché unique numérique. Par conséquent, la communication de crise joue un rôle particulièrement important dans l'atténuation des effets négatifs des incidents et des crises de cybersécurité. La communication peut également être utilisée, dans le contexte du cadre pour une réponse diplomatique conjointe, pour influencer le comportement des agresseurs (potentiels) qui agissent depuis des pays tiers. Il est essentiel, en vue d'une réaction politique efficace, d'harmoniser la communication publique destinée à atténuer les incidents et les crises de cybersécurité et la communication publique destinée à influencer l'agresseur.

(23) La fourniture d'informations au public sur les moyens d'atténuer les effets d'un incident au niveau de l'utilisateur ou de l'organisation (par exemple en appliquant des corrections informatiques ou en prenant des mesures supplémentaires pour éviter la menace, etc.) pourrait être une mesure efficace pour atténuer un incident ou une crise de cybersécurité majeurs.

(24) Par l'intermédiaire de l'infrastructure de services numériques pour la cybersécurité, qui relève du mécanisme pour l'interconnexion en Europe (MIE), la Commission élabore actuellement un mécanisme de coopération sous la forme d'une plateforme de services centrale, appelé MeliCERTes, entre les CSIRT des États membres participants afin d'améliorer leur niveau de préparation, de coopération et de réaction aux menaces et incidents émergents dans le cyberespace. Par des appels à propositions concurrentiels pour l'attribution de subventions au titre du MIE, la Commission cofinance les CSIRT dans les États membres en vue d'améliorer leurs capacités opérationnelles au niveau national.

([1]) En cours d'élaboration; adoption prévue avant la fin de 2017.
([2]) Les lignes directrices devraient être finalisées avant la fin de 2017.
([3]) Conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'Union européenne face aux actes de cybermalveillance («boîte à outils cyberdiplomatique»), document 9916/17.
([4]) Document de travail conjoint des services, Protocole opérationnel de l'Union européenne de lutte contre les menaces hybrides («EU Playbook»), SWD(2016) 227 final, 5 juillet 2016.

(25) Les exercices de cybersécurité au niveau de l'Union européenne sont essentiels pour stimuler et améliorer la coopération entre les États membres et le secteur privé. À cette fin, l'ENISA organise régulièrement depuis 2010 des exercices paneuropéens de simulation de cyberincidents («Cyber Europe»).

(26) Dans ses conclusions ([1]) sur la mise en œuvre de la déclaration commune du président du Conseil européen, du président de la Commission européenne et du secrétaire général de l'Organisation du traité de l'Atlantique Nord (OTAN), le Conseil appelle à renforcer la coopération en matière de cyberexercices, par une participation réciproque des services aux exercices respectifs, notamment Cyber Coalition et Cyber Europe.

(27) L'évolution constante de la nature des menaces et les incidents de cybersécurité survenus récemment trahissent une augmentation du risque auquel l'Union est confrontée, et les États membres devraient donner suite à la présente recommandation dans les plus brefs délais et, en tout état de cause, avant la fin de 2018.

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

(1) Les États membres et les institutions de l'Union européenne devraient créer un cadre de l'Union européenne pour la réaction aux crises de cybersécurité qui intègre les objectifs et les modalités de la coopération présentés dans le plan d'action en suivant les principes directeurs décrits dans ce document.

(2) Le cadre de l'Union européenne pour la réaction aux crises de cybersécurité devrait notamment désigner les acteurs, institutions de l'Union européenne et autorités des États membres concernés, à tous les niveaux requis, à savoir technique, opérationnel, stratégique/politique, et élaborer, en tant que de besoin, des procédures opératoires standards décrivant la manière dont ils coopèrent dans le contexte des mécanismes de gestion de crise de l'Union européenne. Il faut s'attacher en particulier à organiser sans retard l'échange d'informations et à coordonner les réactions lors des incidents et des crises de cybersécurité majeurs.

(3) À cette fin, il convient que les autorités compétentes des États membres travaillent ensemble au développement des protocoles de partage d'informations et de coopération. Le groupe de coopération devrait procéder à des échanges d'expériences sur ces questions avec les institutions concernées de l'Union européenne.

(4) Les États membres devraient veiller à ce que leurs mécanismes nationaux de gestion de crise prennent en charge de manière satisfaisante la réaction aux cyberincidents et prévoient les procédures de coopération nécessaires au niveau de l'Union européenne dans le contexte du cadre de l'Union européenne.

(5) En ce qui concerne les mécanismes de gestion de crise existants de l'Union européenne, conformément au plan d'action, les États membres devraient établir, avec les services de la Commission et le SEAE, des lignes directrices pratiques en ce qui concerne l'intégration de leurs entités et procédures nationales en matière de gestion de crise et de cybersécurité dans les mécanismes de gestion de crise de l'Union européenne, à savoir l'IPCR et le CRM du SEAE. Les États membres devraient notamment veiller à ce que des structures appropriées soient mises en place pour permettre un flux d'informations efficace entre leurs autorités de gestion de crise nationales et leurs représentants au niveau de l'Union européenne dans le contexte des mécanismes de crise de l'Union européenne.

(6) Les États membres devraient faire pleinement usage des possibilités offertes par le programme du mécanisme pour l'interconnexion en Europe (MIE) relatif aux infrastructures de services numériques (DSI) dans le domaine de la cybersécurité et coopérer avec la Commission pour que le mécanisme de coopération sous forme de plateforme de services centrale, qui est actuellement en cours d'élaboration, présente les fonctionnalités requises et réponde à leurs besoins de coopération également lors des crises de cybersécurité.

(7) Les États membres, avec l'aide de l'ENISA et en s'appuyant sur les travaux déjà réalisés dans ce domaine, devraient coopérer pour élaborer et adopter une taxonomie et un modèle communs pour les rapports de situation devant décrire les causes techniques et les incidences des incidents liés à la cybersécurité, de manière à renforcer leur coopération technique et opérationnelle en cas de crise. À cet égard, les États membres devraient tenir compte des travaux en cours au sein du groupe de coopération en ce qui concerne les lignes directrices en matière de notification d'incidents, et notamment les aspects liés au format des notifications nationales.

(8) Les procédures définies dans le cadre devraient être testées et, au besoin, révisées en fonction des enseignements tirés de la participation des États membres aux exercices de cybersécurité aux niveaux national, régional et de l'Union, ainsi qu'aux exercices cyberdiplomatiques et de l'OTAN. Elles devraient notamment être mises à l'épreuve dans le contexte des exercices «CyberEurope» organisés par l'ENISA. CyberEurope 2018 sera la première occasion de procéder à de tels essais.

([1]) Document ST 15283/16 du 6 décembre 2016.

(9) Les États membres et les institutions de l'Union européenne devraient s'exercer régulièrement pour affûter leur réaction aux incidents et aux crises de cybersécurité majeurs à l'échelon national et européen, y compris sur le plan politique, s'il y a lieu, et avec la participation d'entités du secteur privé, le cas échéant.

Fait à Bruxelles, le 13 septembre 2017.

Par la Commission

Mariya GABRIEL

Membre de la Commission

ANNEXE

Plan d'action pour une réaction coordonnée aux incidents et crises transfrontières de cybersécurité majeurs

INTRODUCTION

Le présent plan d'action s'applique aux incidents de cybersécurité qui provoquent des perturbations dépassant les capacités d'action du seul État membre concerné ou qui frappent plusieurs États membres en s'accompagnant de répercussions techniques et politiques si vastes qu'ils requièrent une coordination et une réaction rapides à l'échelle politique dans l'Union.

Les incidents de cette ampleur sont considérés comme des «crises» de cybersécurité.

En cas de crise à l'échelle de l'Union européenne touchant à la cybersécurité, la coordination de la réaction au niveau politique dans l'Union sera assurée par le Conseil au moyen du dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR).

Au sein de la Commission, la coordination s'effectuera dans le cadre du système général d'alerte rapide «ARGUS».

Si la crise comporte d'importantes implications liées à la politique extérieure ou à la politique de sécurité et de défense commune (PSDC), le système de réponse aux crises du Service européen pour l'action extérieure (SEAE) est activé.

Le plan d'action indique comment ces mécanismes bien établis de gestion des crises doivent exploiter pleinement les structures existantes en matière de cybersécurité à l'échelon de l'Union européenne ainsi que les mécanismes de coopération entre les États membres.

Pour ce faire, il tient compte d'un ensemble de principes directeurs (proportionnalité, subsidiarité, complémentarité et confidentialité des informations), en présentant les objectifs essentiels de la coopération (réaction efficace, appréciation commune de la situation, messages destinés au public) à trois niveaux (stratégique/politique, opérationnel et technique), les mécanismes et les acteurs associés ainsi que les activités visant à atteindre ces objectifs.

Le plan d'action ne couvre pas l'ensemble du cycle de gestion de crise (prévention/atténuation, préparation, réaction, retour à la normale); il est axé sur la phase de réaction, mais aborde néanmoins certaines autres activités, en particulier celles liées à l'acquisition d'une appréciation commune de la situation.

Il importe également de noter que les incidents de cybersécurité peuvent être à l'origine ou faire partie d'une crise plus vaste frappant d'autres secteurs. Vu les effets prévisibles de la plupart des crises de cybersécurité sur le monde physique, la réaction qui s'impose, quelle qu'elle soit, doit comprendre des mesures d'atténuation tant intérieures qu'extérieures au cyberespace. Il convient de coordonner ces mesures avec les autres mécanismes de gestion des crises à l'échelon de l'Union européenne, dans les États membres et dans les différents secteurs.

Enfin, le plan d'action ne remplace pas et ne doit pas porter atteinte aux mécanismes, arrangements ou instruments relevant de secteurs ou de politiques spécifiques, tels que le système mondial de navigation par satellite (GNSS) européen ([1]).

Principes directeurs

Les principes directeurs suivants ont servi pour la définition des objectifs, la détermination des activités nécessaires et l'attribution des fonctions et des responsabilités aux différents acteurs et mécanismes, et doivent également être respectés aux fins de l'élaboration des futures lignes directrices pour la mise en œuvre.

Proportionnalité: la grande majorité des incidents de cybersécurité touchant les États membres se situent bien en dessous de ce qui peut être considéré comme une crise «nationale», sans parler d'une crise européenne. La base de la coopération entre les États membres face à de tels incidents est constituée par le réseau des centres de réponse aux incidents de sécurité informatique (CSIRT) institué par la directive SRI ([2]). Les CSIRT nationaux coopèrent et échangent volontairement des informations sur une base journalière y compris, le cas échéant, en réponse à des incidents de cybersécurité qui affectent un ou plusieurs États membres, conformément aux procédures opératoires standards (POS) du réseau des CSIRT. Il convient que le plan d'action tire pleinement parti de ces procédures, en les complétant par des éléments propres aux crises de cybersécurité.

([1]) Décision 2014/496/PESC.
([2]) Directive (UE) 2016/1148.

Subsidiarité: le principe de subsidiarité est essentiel. C'est aux États membres qu'il appartient au premier chef de répondre aux incidents et crises de cybersécurité majeurs qui les touchent. La Commission, le SEAE et d'autres institutions, offices, agences et organes de l'Union européenne ont cependant un rôle important à jouer, expressément prévu dans le dispositif IPCR et qui découle également du droit de l'Union ou tout simplement du fait que les incidents et les crises liés à la cybersécurité peuvent avoir une incidence sur tous les pans de l'activité économique au sein du marché unique, sur la sécurité et les relations internationales de l'Union ainsi que sur les institutions elles-mêmes.

Complémentarité: le plan d'action tient pleinement compte des mécanismes existants de gestion des crises à l'échelon de l'Union européenne, à savoir le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR), le système général d'alerte rapide «ARGUS» et le système de réponse aux crises du SEAE, et intègre les structures et mécanismes nouvellement créés en vertu de la directive SRI, à savoir le réseau des CSIRT, ainsi que les agences et organismes concernés, à savoir l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), le Centre européen de lutte contre la cybercriminalité au sein d'Europol (Europol/EC3), le Centre d'analyse du renseignement de l'Union européenne (INTCEN), la direction «Renseignement» de l'État-major de l'Union européenne (EUMS INT) et la salle de veille (SITROOM) de l'INTCEN, coopérant dans le cadre de la SIAC (capacité unique d'analyse du renseignement); la cellule de fusion de l'Union européenne contre les menaces hybrides (au sein de l'INTCEN); l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne (CERT-UE). Ce faisant, le plan d'action devrait également garantir une complémentarité maximale et une redondance minimale dans l'interaction et la coopération de ces différentes structures.

Confidentialité des informations: tous les échanges d'informations dans le contexte du plan d'action doivent satisfaire aux règles applicables en matière de sécurité et de protection des données à caractère personnel ([1]) ainsi qu'au «Traffic Light Protocol» ([2]). Aux fins de l'échange d'informations classifiées, quel que soit le régime de classification appliqué, il y a lieu d'utiliser les outils agréés disponibles ([3]). En ce qui concerne le traitement des données à caractère personnel, il respectera les règles de l'Union européenne applicables, en particulier le règlement général sur la protection des données ([4]), la directive «vie privée et communications électroniques» ([5]) et le règlement ([6])«relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes, bureaux et agences de l'Union et à la libre circulation de ces données».

Objectifs essentiels

La coopération prévue par le plan d'action se déroule aux trois niveaux mentionnés plus haut: politique, opérationnel et technique. À chacun de ces niveaux, la coopération peut comporter l'échange d'informations ainsi que des actions conjointes, et vise à atteindre les objectifs essentiels suivants.

— Permettre une réponse efficace: cette réponse peut prendre de nombreuses formes, depuis la détermination de mesures techniques, qui peut mobiliser plusieurs entités examinant conjointement les causes techniques de l'incident (par exemple analyse de logiciels malveillants), ou la définition de méthodes permettant aux organisations de déterminer si elles sont touchées (par exemple indicateurs de compromis), jusqu'aux décisions opérationnelles concernant l'application de ces mesures techniques et, au niveau politique, aux décisions d'activation d'autres instruments tels que la réponse diplomatique commune de l'Union européenne face aux actes de cybermalveillance («boîte à outils cyberdiplomatique») ou le protocole opérationnel de l'Union européenne visant à contrer les menaces hybrides, en fonction de l'incident.

— Appréciation commune de la situation: une compréhension suffisamment bonne des événements à mesure de leur déroulement est essentielle pour toutes les parties prenantes aux trois niveaux (technique, opérationnel, politique) pour assurer une réponse coordonnée. L'appréciation de la situation peut inclure des éléments technologiques sur les causes et les origines de l'incident ainsi que sur ses répercussions. Les incidents de cybersécurité pouvant toucher un large éventail de secteurs (finance, énergie, transports, soins de santé, etc.), il est impératif que les informations appropriées, dans un format adéquat, parviennent en temps utile à toutes les parties prenantes.

([1]) Décisions de la Commission (UE, Euratom) 2015/443 du 13 mars 2015 relative à la sécurité au sein de la Commission (JO L 72 du 17.3.2015, p. 41) et (UE, Euratom) 2015/444 du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 72 du 17.3.2015, p. 53); décision de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 19 avril 2013 relative aux règles de sécurité applicables au Service européen pour l'action extérieure (JO C 190 du 29.6.2013, p. 1); décision 2013/488/UE du Conseil du 23 septembre 2013 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 274 du 15.10.2013, p. 1).

([2]) https://www.first.org/tlp/

([3]) En juin 2016, ces canaux de transmission comprenaient les systèmes CIMS (système de gestion des informations classifiées), ACID (algorithme de chiffrement), RUE (système sécurisé pour la création, l'échange et l'archivage des documents RESTREINT UE/EU RESTRICTED) et SOLAN. On peut encore citer les systèmes PGP ou S/MIME.

([4]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

([5]) Directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

([6]) Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1) — en cours de réexamen.

— Convenir des messages essentiels destinés au public ([1]): la communication joue un rôle capital pour atténuer les effets négatifs des incidents et crises de cybersécurité, et peut également servir à influer sur le comportement des agresseurs (potentiels). Un message approprié peut également servir à envoyer un signal clair sur les conséquences probables d'une réponse diplomatique afin d'influer sur le comportement des agresseurs. Pour assurer l'efficacité d'une réponse politique, il est essentiel de coordonner la communication visant à atténuer les effets négatifs des incidents et des crises de cybersécurité et la communication visant à influencer un agresseur. Un élément crucial en matière de cybersécurité est la diffusion d'informations pratiques précises permettant au public d'atténuer les effets d'un incident (par exemple application d'un correctif, actions complémentaires pour se prémunir contre la menace, etc.).

COOPÉRATION ENTRE ÉTATS MEMBRES ET ENTRE LES ÉTATS MEMBRES ET LES ACTEURS DE L'UNION EUROPÉENNE AUX NIVEAUX TECHNIQUE, OPÉRATIONNEL ET STRATÉGIQUE/POLITIQUE

Une réponse efficace face aux incidents ou aux crises de cybersécurité à grande échelle au niveau de l'Union européenne passe par une coopération effective en matière technique, opérationnelle et stratégique/politique.

À chaque niveau, les acteurs impliqués devraient mener des activités spécifiques visant à atteindre trois objectifs essentiels:

— réponse coordonnée,

— appréciation commune de la situation,

— communications publiques.

Tout au long de l'incident ou de la crise, les premiers niveaux de coopération alerteront, informeront et assisteront les niveaux supérieurs qui formuleront des orientations ([2]) et prendront des décisions, selon le cas, à l'intention des premiers niveaux.

Coopération au niveau technique

Champ des activités:

— gestion d'incident ([3]) lors d'une crise de cybersécurité,

— suivi d'incident comprenant l'analyse continue des menaces et des risques.

Acteurs potentiels

Au niveau technique, le mécanisme central de coopération prévu dans le plan d'action est le réseau des CSIRT, sous la direction de la présidence du Conseil et avec le secrétariat fourni par l'ENISA.

— États membres:

  — autorités compétentes et points de contact uniques établis par la directive SRI,

  — CSIRT.

— Organes/bureaux/agences de l'Union européenne:

  — ENISA,

  — Europol/EC3,

  — CERT-EU.

([1]) Il faut noter ici que la communication avec le public peut faire référence à la fois à la communication sur l'incident à l'intention du grand public et à la transmission d'informations à caractère plus technique ou opérationnel à des secteurs critiques et/ou aux parties touchées. Cela peut imposer l'utilisation de canaux de diffusion confidentiels et d'outils ou de plateformes techniques spécifiques. Dans les deux cas, la communication avec les acteurs et le grand public au niveau national appartient à chaque État membre. Ainsi, conformément au principe de subsidiarité évoqué plus haut, les États membres et les CSIRT nationaux ont la responsabilité ultime des informations diffusées sur leur territoire ou à leurs administrés, respectivement.

([2]) «Autorisation d'agir»: en cas de crise de cybersécurité, il est crucial de réagir rapidement pour mettre sur pied les actions d'atténuation appropriées. Afin d'assurer des délais de réaction courts, des «autorisations d'agir» peuvent être délivrées par un État membre à l'intention d'un autre État membre, le premier donnant ainsi au second l'autorisation d'agir immédiatement, sans devoir consulter les niveaux supérieurs ou les institutions de l'Union européenne et sans passer par tous les canaux officiels normalement requis, lorsque cela n'est pas nécessaire dans un incident particulier (par exemple, un CSIRT ne devrait pas avoir à consulter les niveaux supérieurs pour transmettre à un CSIRT dans un autre État membre des informations précieuses).

([3]) On entend par «gestion d'incident» toutes les procédures utiles à la détection, à l'analyse et au confinement d'un incident et toutes les procédures utiles à l'intervention en cas d'incident.

— Commission européenne:

  — l'ERCC [service opérationnel permanent de la direction générale de la protection civile et des opérations d'aide humanitaire européennes (ECHO)] et le service chef de file (soit la direction générale des réseaux de communication, du contenu et des technologies, soit la direction générale de la migration et des affaires intérieures, en fonction de la nature de l'incident), le secrétariat général (SG) (secrétariat du système ARGUS), la direction générale des ressources humaines et de la sécurité et la direction générale de l'informatique (Sécurité informatique — Opérations),

  — pour les autres agences de l'Union européenne ([1]), la direction générale de tutelle de la Commission ou le SEAE (premier point de contact).

— SEAE:

  — SIAC [capacité unique d'analyse du renseignement: centre d'analyse du renseignement de l'Union européenne (INTCEN) et direction «Renseignement» de l'État-major de l'Union européenne (EUMS INT)],

  — salle de veille de l'Union européenne et service géographique ou thématique désigné,

  — cellule de fusion de l'Union européenne contre les menaces hybrides (au sein de l'INTCEN — cybersécurité dans un contexte hybride).

Appréciation commune de la situation

— Dans le cadre de la coopération régulière au niveau technique en vue de l'acquisition d'une appréciation de la situation commune à toute l'Union, l'ENISA devrait établir périodiquement un rapport technique sur la situation dans l'Union européenne en matière de cybersécurité relatif aux incidents et menaces, fondé sur les informations accessibles au public, sur sa propre analyse et sur les rapports que lui ont communiqués les CSIRT des États membres (sur une base volontaire) ou les points de contact uniques prévus par la directive SRI, le Centre européen de lutte contre la cybercriminalité au sein d'Europol (Europol/EC3) et la CERT-UE, et, le cas échéant, le Centre d'analyse du renseignement de l'Union européenne (INTCEN) au Service européen pour l'action extérieure (SEAE). Ce rapport devrait être mis à la disposition des instances concernées du Conseil, de la Commission, du haut représentant et du réseau des CSIRT.

— En cas d'incident grave, la présidence du réseau des CSIRT, assistée de l'ENISA, prépare un rapport sur la situation incidentelle de cybersécurité dans l'Union européenne ([2]) qui est remis à la présidence du Conseil, à la Commission et à la HRVP par l'intermédiaire du CSIRT de l'État membre assurant la présidence tournante.

— *Toutes les autres agences de l'Union européenne* font rapport à leurs directions générales (DG) de tutelle respectives, qui font à leur tour rapport au service chef de file de la Commission.

— La *CERT-UE* fournit des rapports techniques au réseau des CSIRT, aux institutions et agences de l'Union européenne (selon le cas) et au système ARGUS (s'il est activé).

— *Europol/EC3* ([3]) *et la CERT-UE* fournissent au réseau des CSIRT des expertises criminalistiques d'éléments techniques ainsi que d'autres informations techniques.

— SIAC-SEAE: pour le compte de l'INTCEN, la cellule de fusion de l'Union européenne contre les menaces hybrides fait rapport aux services concernés du SEAE.

Réaction

— *Le réseau des CSIRT* communique des précisions et des analyses techniques concernant l'incident, tels que des adresses IP, des indicateurs de compromis ([4]) etc. Ces informations devraient être transmises sans délai à l'ENISA et au plus tard 24 heures après la détection de l'incident.

— Conformément aux procédures opératoires standards du réseau des CSIRT, les membres de ce réseau coopèrent dans le cadre de leurs efforts d'analyse des éléments techniques disponibles et d'autres informations techniques liées à l'incident, en vue d'en déterminer la cause et de définir les mesures techniques d'atténuation envisageables.

— L'ENISA aide les CSIRT dans leurs activités techniques en s'appuyant sur son expertise et conformément à son mandat ([5]).

([1]) En fonction de la nature et de l'impact de l'incident sur les différents secteurs d'activité (finance, transports, énergie, soins de santé, etc.), les agences ou organes concernés de l'Union européenne seront saisis.

([2]) Ce rapport est établi à partir des rapports nationaux remis par les CSIRT nationaux. Le format que doit respecter ce rapport devrait être décrit dans les procédures opératoires standards du réseau des CSIRT.

([3]) Conformément au cadre légal d'EC3, dans les conditions et selon les procédures qu'il prévoit.

([4]) En criminalistique informatique, on entend par «indicateur de compromis» un élément observé sur un réseau ou dans un système d'exploitation qui indique avec un indice de confiance élevé une intrusion informatique. Les indicateurs de compromis les plus courants sont des signatures de virus et des adresses IP, des empreintes MD5 de fichiers de logiciels malveillants, des URL et des noms de domaine de serveurs de commande et contrôle de botnets.

([5]) Proposition de règlement relatif à l'ENISA, l'Agence européenne de cybersécurité et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification de la cybersécurité des technologies de l'information et des communications («règlement sur la cybersécurité»), 13 septembre 2017.

— Les CSIRT des États membres coordonnent leurs activités de réponse technique avec l'aide de l'ENISA et de la Commission.

— SIAC-SEAE: pour le compte de l'INTCEN, la cellule de fusion de l'Union européenne contre les menaces hybrides lance le processus de collecte des premiers éléments de preuve.

Communications publiques

— Les CSIRT élaborent des conseils techniques ([1]) et des alertes de vulnérabilité ([2]) et les diffusent auprès de leurs communautés respectives et du public selon les procédures d'autorisation applicables dans chaque cas.

— L'ENISA facilite la production et la diffusion des communications communes du réseau des CSIRT.

— L'ENISA coordonne ses activités de communication publique avec le réseau des CSIRT et le service du porte-parole de la Commission.

— L'ENISA et l'EC3 coordonnent leurs activités de communication publique sur la base de l'appréciation commune de la situation convenue entre les États membres. Ils coordonnent tous deux leurs activités de communication publique avec le service du porte-parole de la Commission.

— Si la crise comporte une dimension extérieure ou touchant à la politique de défense et de sécurité commune, il convient de coordonner la communication publique avec le SEAE et le service du porte-parole du haut représentant.

Coopération au niveau opérationnel

Champ des activités

— Élaborer le processus de décision au niveau politique

— Coordonner la gestion de la crise de cybersécurité (le cas échéant)

— Évaluer les conséquences et l'impact au niveau de l'Union européenne et proposer des mesures d'atténuation éventuelles

Acteurs potentiels

— États membres:

  — autorités compétentes et points de contact uniques créés en vertu de la directive SRI,

  — CSIRT, organismes chargés de la cybersécurité,

  — autorités sectorielles nationales (en cas d'incident ou de crise touchant plusieurs secteurs).

— Organes/bureaux/agences de l'Union européenne:

  — ENISA,

  — Europol/EC3,

  — CERT-EU.

— Commission européenne:

  — secrétaire général (adjoint) SG (système ARGUS),

  — directions générales des réseaux de communication, du contenu et des technologies/de la migration et des affaires intérieures,

  — autorité de sécurité de la Commission,

  — autres directions générales (en cas d'incident ou de crise touchant plusieurs secteurs).

([1]) Conseils à caractère technique concernant les causes de l'incident et les actions d'atténuation possibles.
([2]) Informations sur la vulnérabilité technique exploitée pour nuire aux systèmes informatiques.

— SEAE:

  — secrétaire général (adjoint) pour la réaction aux crises et SIAC (EU INTCEN et EUMS INT),

  — cellule de fusion de l'Union européenne contre les menaces hybrides.

— Conseil

  — présidence [présidence du groupe horizontal «Questions liées au cyberespace» ou Coreper ([1])] avec l'appui du secrétariat général du Conseil (SGC) ou du Comité politique et de sécurité (COPS) ([2]) et — s'il est activé — avec l'appui du dispositif IPCR.

Appréciation de la situation

— Soutenir la production de rapports sur la situation politico-stratégique [par exemple l'Integrated Situational Awareness and Analysis (ISAA) en cas d'activation du dispositif IPCR]

— Le *groupe horizontal «Questions liées au cyberespace» du Conseil* prépare les réunions du Coreper ou du COPS, selon le cas.

— En cas d'activation du dispositif IPCR:

  — la présidence peut convoquer des tables rondes pour l'aider à préparer les réunions du Coreper ou du COPS avec la participation des acteurs concernés dans les États membres, des institutions, des agences, de tiers tels que les pays tiers et des organisations internationales. Il s'agit de réunions de crise destinées à repérer les goulets d'étranglement et à élaborer des propositions d'action pour les questions transversales,

  — le *service de la Commission chef de file ou le SEAE* en tant que chef de file pour l'ISAA élabore le rapport ISAA en tenant compte des contributions de l'ENISA, du réseau des CSIRT, d'Europol/EC3, de l'EUMS INT, de l'INTCEN et de tous les autres acteurs concernés. Le rapport ISAA est une évaluation à l'échelle de l'Union européenne fondée sur la corrélation entre les incidents techniques et l'évaluation des crises (analyse des menaces, analyse des risques, conséquences et effets non techniques, aspects de l'incident ou de la crise non liés au cyberespace, etc.) et adaptée aux besoins du niveau opérationnel et du niveau politique.

— En cas d'activation du système ARGUS:

  — la CERT-UE et l'EC3 ([3]) contribuent directement à l'échange d'informations au sein de la Commission.

— En cas d'activation du système de réponse aux crises du SEAE:

  — la SIAC intensifiera sa collecte d'informations, agrégera les informations provenant de toutes les sources et élaborera une analyse et une évaluation de l'incident.

Réaction (à la demande du niveau politique)

— Coopération transfrontière avec le point de contact unique et les autorités nationales compétentes (directive SRI) pour atténuer les conséquences et les effets

— Activation de toutes les mesures techniques d'atténuation et coordination des capacités techniques nécessaires pour stopper ou réduire l'impact des attaques sur les systèmes d'information visés

— Coopération et, si la décision est prise, coordination des capacités techniques en vue d'une réponse conjointe ou collaborative conformément aux ***POS du réseau des CSIRT***

— Évaluation de la nécessité de coopérer avec les tiers concernés

— Processus de décision au sein du système ARGUS (en cas d'activation)

— Élaboration de décisions et coordination dans le cadre du dispositif IPCR (en cas d'activation)

— Appui au processus de décision du SEAE par l'intermédiaire du mécanisme de réaction aux crises du SEAE (en cas d'activation), y compris en ce qui concerne les contacts avec les pays tiers et les organisations internationales ainsi que toute mesure visant à protéger les missions et opérations de la PSDC et les délégations de l'Union européenne

([1]) Le Comité des représentants permanents ou Coreper (article 240 du traité sur le fonctionnement de l'Union européenne — TFUE) est chargé de préparer les travaux du Conseil de l'Union européenne.

([2]) Le Comité politique et de sécurité est un comité du Conseil de l'Union européenne chargé de la politique étrangère et de sécurité commune (PESC) mentionné à l'article 38 du traité sur l'Union européenne.

([3]) Dans le respect et en vertu des conditions et procédures définies dans le cadre juridique régissant l'EC3.

Communications publiques

— Mise au point concertée des messages adressés au public sur l'incident

— Si la crise comporte des implications liées à la politique extérieure ou à la politique de sécurité et de défense commune (PSDC), la communication au public devrait être coordonnée au sein du SEAE et du service du porte-parole du haut représentant.

Coopération au niveau stratégique/politique

Acteurs potentiels

— Pour les États membres, les ministres chargés de la cybersécurité

— Pour le Conseil européen, le président

— Pour le Conseil, la présidence tournante

— Pour les mesures relevant de la «boîte à outils cyberdiplomatique», le COPS et le groupe horizontal

— Pour la Commission européenne, le président ou le vice-président/commissaire délégué

— Le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité/vice-président de la Commission

Champ des activités: gestion stratégique et politique des aspects de la crise tant liés que non liés au cyberespace, y compris les mesures relevant du cadre pour une réponse conjointe face aux actes de cybermalveillance.

Appréciation commune de la situation

— Détermination des incidences des perturbations provoquées par la crise sur le fonctionnement de l'Union

Réaction

— Activer des mécanismes/instruments de gestion de crise supplémentaires, en fonction de la nature et de l'impact de l'incident. Il peut s'agir, par exemple, du mécanisme de protection civile

— Prendre des mesures au titre du cadre pour une réponse diplomatique conjointe de l'Union européenne face aux actes de cybermalveillance

— Mettre une aide d'urgence à la disposition des États membres touchés en activant, par exemple, le fonds d'intervention d'urgence en matière de cybersécurité ([1]) lorsque les conditions seront réunies

— Coopération et coordination avec les organisations internationales, le cas échéant, telles que l'Organisation des Nations unies (ONU), l'Organisation pour la sécurité et la coopération en Europe (OSCE) et, tout particulièrement, l'Organisation du traité de l'Atlantique Nord (OTAN)

— Analyser les implications dans le domaine de la défense et de la sécurité nationale

Communications publiques

Arrêter une stratégie de communication commune envers le public

RÉACTION COORDONNÉE AVEC LES ÉTATS MEMBRES AU NIVEAU DE L'UNION EUROPÉENNE DANS LE CADRE DU DISPOSITIF IPCR

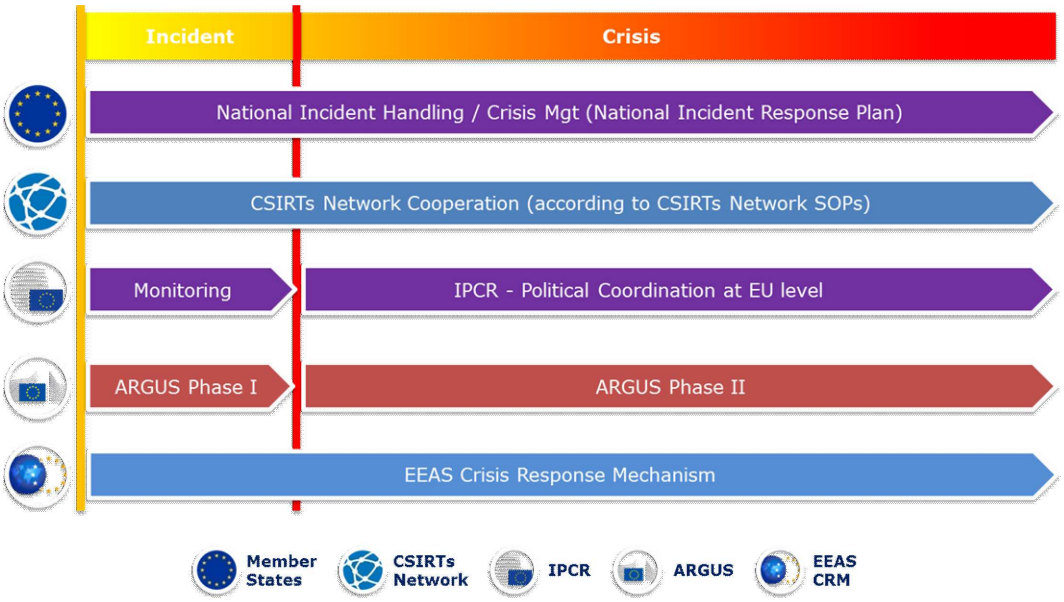
Dans le respect du principe de complémentarité au niveau de l'Union européenne, le présent point se concentre sur l'objectif central et les responsabilités et activités des autorités des États membres, du réseau des CSIRT, de l'ENISA, de la CERT-UE, d'Europol/EC3, de l'INTCEN, de la cellule de fusion de l'Union européenne contre les menaces hybrides et du groupe horizontal «Questions liées au cyberespace» du Conseil dans le cadre du dispositif IPCR. Les acteurs sont supposés agir conformément aux procédures fixées à l'échelon de l'Union européenne ou à l'échelon national.

Il est essentiel de garder à l'esprit que, comme l'illustre la figure 1, indépendamment de l'activation des mécanismes de gestion de crise de l'Union européenne, les activités à l'échelon national et la coopération au sein du réseau des CSIRT (s'il y a lieu) se déroulent, du début à la fin d'un incident ou d'une crise, suivant les principes de subsidiarité et de proportionnalité.

([1]) Communication conjointe «Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide», JOIN(2017) 450/1.

Figure 1

Réaction à un incident/une crise de cybersécurité au niveau de l'Union européenne



Toutes les activités décrites ci-après doivent respecter les procédures opératoires standards et les règles des mécanismes de coopération concernés ainsi que les mandats et compétences assignés aux différents acteurs et institutions. Ces procédures et ces règles peuvent nécessiter des ajouts ou des modifications pour assurer une coopération optimale et une réaction efficace face aux crises et incidents de cybersécurité majeurs.

Si les acteurs présentés ci-dessous ne sont pas tous tenus d'intervenir à chaque fois qu'un incident se produit, le plan d'action et les procédures opératoires standards applicables se doivent de prévoir leur participation éventuelle.

Compte tenu des répercussions variables que peut avoir un incident ou une crise de cybersécurité sur la société, il faudra assurer une grande souplesse dans l'intervention des acteurs de chaque secteur à tous les niveaux et veiller à une réaction appropriée en recourant à des activités d'atténuation aussi bien liées que non liées au cyberespace.

Gestion de crise dans le domaine de la cybersécurité — Intégration de la cybersécurité dans le dispositif IPCR

Le dispositif IPCR, tel qu'il est décrit dans les POS de l'IPCR ([1]), suit l'ordre des étapes ci-dessous (la réalisation de certaines de ces étapes dépendra de la situation).

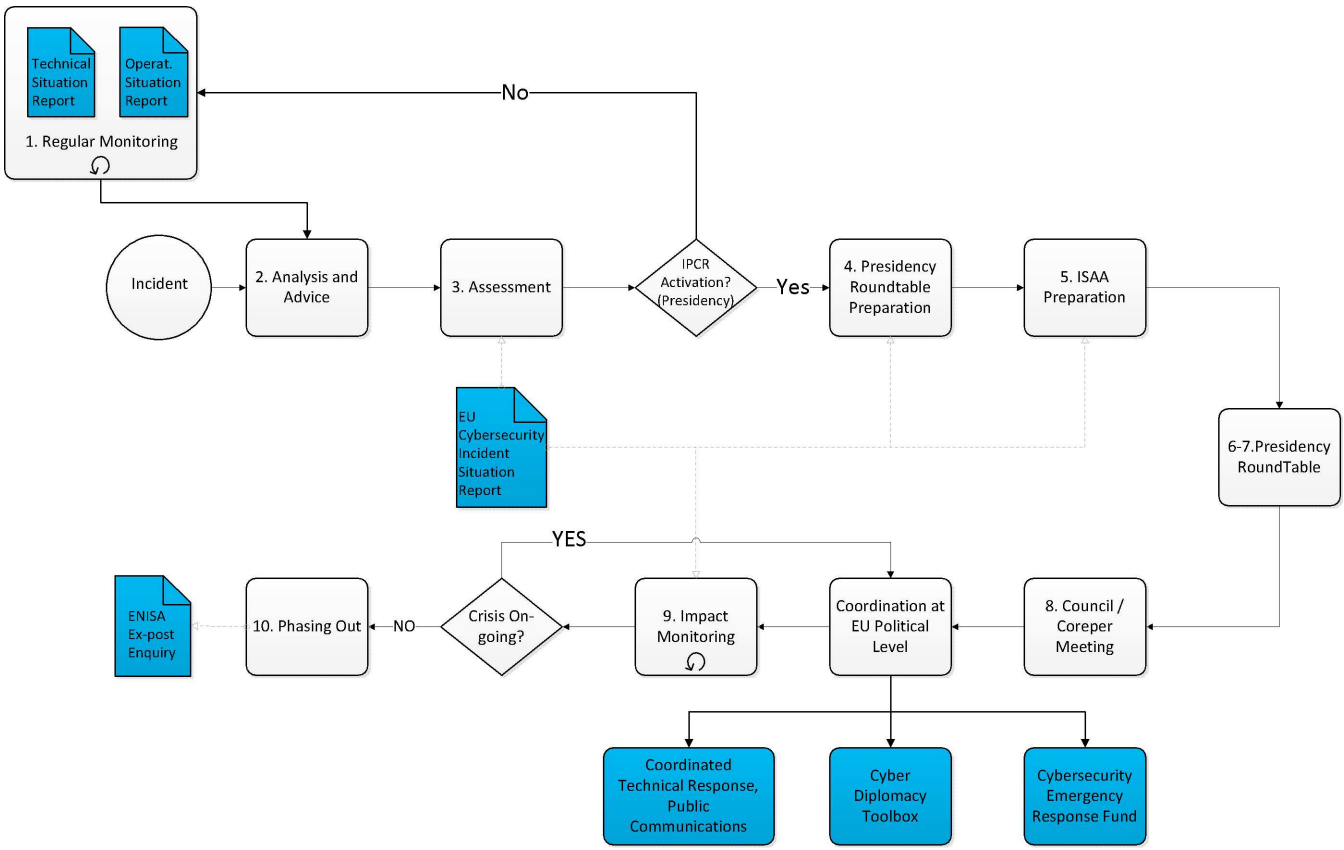
À chaque étape, nous indiquons les activités et les acteurs spécifiquement concernés par la cybersécurité. Par commodité de lecture, le texte des POS de l'IPCR est fourni à chaque étape, suivi des activités spécifiques prévues par le plan d'action. Cette approche par étapes permet également de repérer avec précision les **lacunes** que présentent les capacités et procédures nécessaires et qui nuisent à l'efficacité de la réaction aux crises de cybersécurité.

La figure 2 ci-dessous ([2]) offre une représentation graphique du dispositif IPCR dans laquelle les nouveaux éléments en cours d'introduction sont surlignés en bleu.

([1]) Voir le document 12607/15 «Procédures opératoires standard IPCR», approuvé par le groupe des Amis de la présidence, dont le Coreper a pris note en octobre 2015.
([2]) On trouvera dans l'appendice une version agrandie de la figure.

Figure 2

Éléments spécifiques à la cybersécurité dans l'IPCR



Remarque: compte tenu de la nature des menaces hybrides dans le cyberespace qui ne présentent pas nécessairement le caractère d'une crise avérée, l'Union européenne doit prendre des mesures de prévention et de préparation. La cellule de fusion de l'Union européenne contre les menaces hybrides est chargée d'analyser rapidement les incidents concernés et d'informer les structures de coordination appropriées. Les rapports réguliers soumis par la cellule de fusion peuvent contribuer à éclairer les politiques sectorielles de manière à améliorer l'état de préparation.

— **Étape 1 — Surveillance sectorielle régulière et dispositifs d'alerte:** les rapports de situation sectoriels réguliers et les dispositifs d'alerte déjà prévus fournissent des indications à la présidence du Conseil sur les crises naissantes et leur évolution possible.

  — **Lacune relevée:** il n'est pas prévu, à l'heure actuelle, de rapports de situation réguliers et coordonnés et de dispositifs d'alerte concernant les incidents (et menaces) de cybersécurité au niveau de l'Union européenne.

  — **Plan d'action: surveillance/rapports de situation en matière de cybersécurité au niveau de l'Union européenne**

    — L'ENISA élaborera **un rapport de situation technique régulier au niveau de l'Union européenne** sur les incidents et les menaces de cybersécurité, en se fondant sur les informations accessibles au public, sur sa propre analyse et sur les rapports qui lui sont communiqués par les CSIRT des États membres (sur une base volontaire) ou les points de contact uniques prévus par la directive SRI, le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol, la CERT-UE et le Centre du renseignement de l'Union européenne (INTCEN) au sein du Service européen pour l'action extérieure (SEAE). Ce rapport devrait être mis à la disposition des instances concernées du Conseil, de la Commission et du réseau des CSIRT.

    — Pour le compte de la SIAC, la cellule de fusion de l'Union européenne contre les menaces hybrides devrait élaborer un **rapport de situation opérationnelle sur la cybersécurité au niveau de l'Union européenne**. Ce rapport sert également aux fins du cadre pour une réponse diplomatique conjointe de l'Union européenne face aux actes de cybermalveillance.

    — Les deux rapports sont diffusés aux acteurs concernés de l'Union européenne et des États membres pour contribuer à leur appréciation de la situation, éclairer la prise de décision et faciliter la coopération régionale transfrontière.

Après détection d'un incident

— **Étape 2 — Analyse et conseils:** sur la base des données de surveillance et des alertes disponibles, la Commission, le SEAE et le SGC s'informent mutuellement sur l'évolution à prévoir pour être prêts à conseiller la présidence quant à une éventuelle activation (en mode intégral ou en mode de partage d'informations) de l'IPCR.

— **Plan d'action:**

— Pour la Commission, les directions générales des réseaux de communication, du contenu et des technologies, de la migration et des affaires intérieures, des ressources humaines et de la sécurité (direction «Sécurité»), et de l'informatique, avec l'appui de l'ENISA, de l'EC3 et de la CERT-UE.

— SEAE. En se fondant sur les travaux du SITROOM et sur les sources de renseignement, la cellule de fusion de l'Union européenne contre les menaces hybrides fournit des éléments d'appréciation de la situation quant aux menaces hybrides réelles ou potentielles pesant sur l'Union européenne et ses partenaires, y compris les cybermenaces. Par conséquent, lorsque l'analyse et l'évaluation de la cellule de fusion de l'Union européenne contre les menaces hybrides indiquent l'existence d'éventuelles menaces dirigées contre un État membre, des pays partenaires ou une organisation, les informations de l'INTCEN se situeront (en premier ressort) sur le plan opérationnel, conformément aux procédures établies. Ensuite, le niveau opérationnel élaborera des recommandations pour le niveau politico-stratégique, parmi lesquelles l'activation éventuelle de mécanismes de gestion de crise en mode de surveillance (par exemple le système de réponse aux crises du SEAE et la page de l'IPCR relative à la surveillance).

— La présidence du réseau des CSIRT, assistée de l'ENISA, prépare un rapport sur la situation incidentelle de cybersécurité dans l'Union européenne ([1]), qui est remis à la présidence du Conseil, à la Commission et au haut représentant par l'intermédiaire du CSIRT de l'État membre assurant la présidence tournante.

— **Étape 3 — Évaluation/décision sur l'activation de l'IPCR:** la présidence du Conseil évalue la nécessité d'une coordination politique, d'un échange d'informations ou d'une prise de décision au niveau de l'Union européenne. À cette fin, elle peut convoquer une table ronde informelle. Elle procède à une première identification des domaines nécessitant l'implication du Coreper ou du Conseil. Il en résultera un cadre de base pour l'élaboration de rapports ISAA (Integrated Situational Awareness and Analysis). La présidence du Conseil décidera, au vu des caractéristiques de la crise, de ses conséquences éventuelles et des impératifs politiques s'y rapportant, s'il convient de convoquer des réunions des groupes de travail du Conseil et/ou du Coreper et/ou du COPS.

— **Plan d'action:**

— Participants aux tables rondes:

— Les services de la Commission et le SEAE conseilleront la présidence en ce qui concerne leurs domaines de compétence respectifs.

— Les représentants des États membres au groupe horizontal «Questions liées au cyberespace», assistés par des experts des capitales (CSIRT, autorités compétentes pour la cybersécurité, autres).

— Orientations politiques/stratégiques pour les rapports ISAA sur la base du dernier rapport de situation de l'Union européenne sur les incidents de cybersécurité et des informations supplémentaires fournies par les participants aux tables rondes.

— Groupes de travail et comités concernés:

— Groupe horizontal «Questions liées au cyberespace».

La Commission, le SEAE et le SGC, en plein accord et en association avec la présidence, peuvent également décider d'activer l'IPCR en mode de partage d'informations en créant une page consacrée à la crise, afin de préparer une éventuelle activation en mode intégral.

— **Étape 4 — Activation de l'IPCR/Collecte et échange d'informations:** au moment de l'activation (que ce soit en mode de partage d'informations ou en mode intégral), une page consacrée à la crise est créée sur la plateforme web de l'IPCR, permettant des échanges d'informations spécifiques sur les aspects importants pour l'ISAA et la préparation des discussions au niveau politique. Le service chef de file pour l'ISAA (un des services de la Commission ou le SEAE) sera désigné en fonction des circonstances de l'événement.

— **Étape 5 — Établissement des rapports ISAA:** l'établissement des rapports ISAA sera lancé. La Commission/le SEAE publiera des rapports ISAA, comme indiqué dans les procédures opératoires standards (POS) ISAA et pourra

([1]) Ce rapport est établi à partir des rapports nationaux remis par les CSIRT nationaux. Le format que doit respecter ce rapport devrait être décrit dans les POS du réseau des CSIRT.

encourager davantage l'échange d'informations sur la plateforme web de l'IPCR ou émettre des demandes d'informations spécifiques. Les rapports ISAA seront adaptés aux besoins de l'échelon politique (c'est-à-dire le Coreper ou le Conseil) définis par la présidence du Conseil et figurant dans ses orientations, permettant ainsi d'avoir un aperçu stratégique de la situation et une discussion éclairée sur les points à l'ordre du jour définis par la présidence. Conformément aux POS ISAA, la nature de la crise dans le domaine de la cybersécurité déterminera qui, des services de la Commission (direction générale des réseaux de communication, du contenu et des technologies, direction général de la migration et des affaires intérieures) ou du SEAE, préparera le rapport ISAA.

À la suite de l'activation de l'IPCR, la présidence précisera les domaines sur lesquels devra spécifiquement porter l'ISAA pour pouvoir faciliter la coordination politique et/ou le processus décisionnel au sein du Conseil. La présidence précisera également le calendrier du rapport après consultation des services de la Commission/du SEAE.

— **Plan d'action:**

— Le rapport ISAA tient compte des contributions des services compétents, notamment:

— le réseau des CSIRT, sous la forme du rapport de situation sur les incidents de cybersécurité,

— EC3, SITROOM, la cellule de fusion de l'Union européenne contre les menaces hybrides, la CERT-UE. La cellule de fusion de l'Union européenne contre les menaces hybrides soutiendra par ses contributions le service chef de file pour l'ISAA et la table ronde de l'IPCR, le cas échéant,

— les agences et organes sectoriels de l'Union européenne en fonction des secteurs touchés,

— les autorités des États membres (autres que les CSIRT).

— Rassembler les contributions aux fins de l'ISAA ([1]):

— Commission et agences de l'Union européenne: le système informatique ARGUS constituera le réseau central interne pour l'ISAA. Les agences de l'Union européenne devront envoyer leurs contributions à leur direction générale de tutelle, qui à son tour entrera les informations utiles dans le système ARGUS. Les services de la Commission et les agences recueilleront les informations auprès des réseaux sectoriels existants des États membres et des organisations internationales, et auprès d'autres sources pertinentes,

— pour le SEAE: la salle de veille de l'Union européenne, avec l'appui des autres départements compétents du SEAE, constituera le réseau central interne et le point de contact unique aux fins de l'ISAA. Le SEAE rassemblera les informations auprès des pays tiers et des organisations internationales compétentes.

— **Étape 6 — Préparation de la table ronde informelle organisée par la présidence:** la présidence, assistée par le secrétariat général du Conseil, établira le calendrier, l'ordre du jour, la liste des participants et les résultats attendus (éventuels objectifs à atteindre) de la table ronde informelle de la présidence. Le secrétariat général du Conseil relaiera les informations pertinentes sur la plateforme web de l'IPCR au nom de la présidence et établira, notamment, l'invitation à la réunion.

— **Étape 7 — Table ronde de la présidence/mesures préparatoires pour la coordination politique/la prise de décision au niveau de l'Union européenne:** la présidence organisera une table ronde informelle afin d'examiner la situation et de préparer et d'étudier les points devant être portés à l'attention du Coreper ou du Conseil. La table ronde informelle de la présidence servira aussi d'enceinte pour l'élaboration, l'examen et la discussion de toutes les propositions d'action à soumettre au Coreper/Conseil.

— **Plan d'action:**

— le groupe horizontal «Questions liées au cyberespace» du Conseil devrait préparer le COPS ou le Coreper.

— **Étape 8 — Coordination politique et prise de décision au niveau du Coreper/Conseil:** les réunions du Coreper/Conseil ont pour finalité de coordonner les mesures de réaction à tous les niveaux, de prendre des décisions concernant des mesures exceptionnelles, de faire des déclarations politiques, etc. Ces décisions constituent également des orientations politiques/stratégiques actualisées pour l'élaboration future des rapports ISAA.

— **Plan d'action:**

— la décision politique visant à coordonner les réponses en cas de crise dans le domaine de la cybersécurité est mise en œuvre grâce à des activités (exécutées par les protagonistes ad hoc) décrites au point 1 relatif à la coopération stratégique/politique, opérationnelle et technique en ce qui concerne la **réaction** et la **communication publique**,

— l'établissement des rapports ISAA se poursuit sur la base d'une coopération sur les plans technique, opérationnel et politique/stratégique en ce qui concerne l'**appréciation de la situation** également décrite au point 1 ci-dessus.

([1]) POS ISAA.

— **Étape 9 — Suivi des conséquences:** le service chef de file pour l'ISAA, assisté des parties apportant leurs contributions à l'ISAA, fournira des informations concernant l'évolution de la crise et les incidences des décisions prises au niveau politique. Ce circuit de retour d'information viendra à l'appui d'un processus évolutif et de la décision de la présidence de poursuivre la participation de l'Union européenne au niveau politique ou de procéder à la désactivation progressive de l'IPCR.

— **Étape 10 — Désactivation progressive:** suivant la même procédure que pour l'activation, la présidence peut convoquer une réunion de la table ronde informelle pour décider s'il convient de maintenir l'IPCR actif ou non. La présidence peut décider de désactiver ou d'abaisser le niveau d'activation.

— **Plan d'action:**

— l'ENISA peut être invitée à contribuer à, ou à mener, une enquête technique a posteriori sur l'incident conformément aux dispositions de son mandat.

APPENDICE

1. GESTION DES CRISES, MÉCANISMES DE COOPÉRATION ET ACTEURS AU NIVEAU DE L'UNION EUROPÉENNE

Mécanismes de gestion des crises

Dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR): le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR) approuvé par le Conseil le 25 juin 2013 ([1]) a pour objet de faciliter une coordination et une réaction rapides à l'échelle politique dans l'Union dans les situations de crise majeure. L'IPCR soutient également la coordination à l'échelon politique de la réponse à une invocation de la clause de solidarité (article 222 du TFUE), telle que définie dans la décision 2014/415/UE du Conseil concernant les modalités de mise en œuvre par l'Union de la clause de solidarité adoptée le 24 juin 2014. Les procédures opératoires standards (POS) ([2]) du dispositif IPCR définissent le processus d'activation et les mesures à prendre par la suite.

ARGUS: système de coordination en cas de crise mis en place par la Commission européenne en 2005 afin de disposer d'une procédure de coordination spécifique en cas de crise majeure de nature multisectorielle. Il est complété par un système général d'alerte rapide (outil informatique) portant le même nom. ARGUS prévoit deux phases: la phase II (en cas de crise multisectorielle majeure) déclenche l'organisation de réunions du comité de coordination de crise (CCC) placé sous l'autorité du président de la Commission ou d'un commissaire auquel cette responsabilité a été confiée. Le CCC rassemble des représentants des directions générales de la Commission, des cabinets et d'autres services de l'Union européenne concernés afin qu'ils dirigent et coordonnent la réaction de la Commission à la crise. Le CCC, qui est présidé par le secrétaire général adjoint, évalue la situation, envisage les options et prend des décisions pragmatiques en ce qui concerne les outils et instruments de l'Union européenne relevant de la responsabilité de la Commission, et s'assure que les décisions sont mises en œuvre ([3]) ([4]).

Système de réponse aux crises du SEAE (CRM): le système de réponse aux crises du SEAE est un système structuré permettant à ce dernier de réagir aux crises et aux situations d'urgence de nature externe ou présentant une dimension extérieure importante — y compris les menaces hybrides — potentiellement ou réellement néfastes pour les intérêts de l'Union européenne ou pour ceux de tout État membre. En assurant la participation des fonctionnaires compétents de la Commission et du secrétariat du Conseil à ses réunions, le CRM facilite la synergie entre les actions entreprises au niveau diplomatique, de la sécurité et de la défense et les instruments financiers, commerciaux et de coopération gérés par la Commission. La cellule de crise peut être activée pendant la durée de la crise.

Mécanismes de coopération

Réseau des CSIRT: le réseau des centres de réponse aux incidents de sécurité informatique regroupe tous les CSIRT nationaux et gouvernementaux et la CERT-UE. La finalité du réseau est de mettre en place et de développer le partage d'informations entre les CSIRT sur les menaces et les incidents liés à la cybersécurité, et également de permettre une coopération dans les réactions aux incidents et aux crises de cybersécurité.

Groupe de travail horizontal «Questions liées au cyberespace» du Conseil: le groupe de travail a été institué en vue d'assurer la coordination stratégique et horizontale des questions relatives à la politique du cyberespace au sein du Conseil et peut être sollicité pour des activités aussi bien législatives que non législatives.

Acteurs

ENISA: l'Agence européenne chargée de la sécurité des réseaux et de l'information a été créée en 2004. Elle travaille en collaboration étroite avec les États membres et le secteur privé en vue de formuler des avis et solutions sur des questions telles que les exercices paneuropéens de cybersécurité, le développement de stratégies nationales de cybersécurité, la coopération entre les CSIRT et le renforcement des capacités. L'ENISA collabore directement avec les CSIRT dans l'Union européenne et assure le secrétariat du réseau des CSIRT.

CCRE: le Centre de coordination de la réaction d'urgence de la Commission européenne (placé sous la responsabilité de la direction générale de l'aide humanitaire et de la protection civile — DG ECHO) soutient et coordonne un large éventail d'activités de prévention, de préparation et de réaction sur une base permanente (24 heures sur 24, 7 jours sur 7). Inauguré en 2013, il sert de plateforme pour les réactions de la Commission face aux crises (en liaison avec d'autres centres de crise de l'Union européenne), notamment comme point de contact central de l'IPCR (24 heures sur 24, 7 jours sur 7).

([1]) 10708/13 sur l'«Achèvement du processus de réexamen du dispositif de coordination dans les situations d'urgence et de crise (CCA): le dispositif intégré pour une réaction au niveau politique dans les situations de crise», approuvé par le Conseil le 24 juin 2013.
([2]) 12607/15, «Procédures opératoires standard IPCR», approuvé par le groupe des Amis de la présidence, dont le Coreper a pris note en octobre 2015.
([3]) Dispositions de la Commission relatives au système d'alerte rapide global «ARGUS», COM(2005) 662 final du 23 décembre 2005.
([4]) Décision 2006/25/CE, Euratom de la Commission du 23 décembre 2005 modifiant son règlement intérieur (JO L 19 du 24.1.2006, p. 20), sur la création du système général d'alerte rapide ARGUS.

Europol/EC3: le Centre européen de lutte contre la cybercriminalité au sein d'Europol (Europol/EC3) inauguré en 2013 soutient la réaction des services répressifs à la cybercriminalité dans l'Union européenne. L'EC3 offre un soutien analytique et opérationnel aux enquêtes des États membres et sert de plateforme pour les informations et les renseignements sur la criminalité à l'appui des opérations et enquêtes des États membres, grâce à des moyens d'analyse, de coordination et d'expertise, ainsi que des moyens techniques et numériques de police scientifique très spécialisés.

CERT-UE: l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union européenne a pour mission d'améliorer la protection des institutions, organes et agences de l'Union européenne contre les menaces dans le cyberespace. Elle appartient au réseau des CSIRT. Elle a conclu des arrangements techniques pour le partage d'informations sur les menaces dans le cyberespace avec la Capacité OTAN de réaction aux incidents informatiques (NCIRC), quelques pays tiers et les principaux acteurs commerciaux dans le domaine de la cybersécurité.

La communauté du renseignement de l'Union européenne comprend le Centre d'analyse du renseignement de l'Union européenne (**INTCEN**) et la direction «Renseignement» de l'État-major de l'Union européenne (**EUMS INT**), qui coopèrent dans le cadre de la **SIAC** (capacité unique d'analyse du renseignement). La mission de la SIAC est de fournir au haut représentant de l'Union pour les affaires étrangères et la politique de sécurité et au SEAE des analyses dans le domaine du renseignement et une appréciation de la situation, ainsi que d'émettre des alertes rapides à leur intention. La SIAC offre ses services aux différents organes de décision de l'Union européenne en matière de politique étrangère et de sécurité commune (PESC), de politique de sécurité et de défense commune (PSDC) et de lutte contre le terrorisme, ainsi qu'aux États membres. L'INTCEN et l'EUMS INT ne sont pas des agences opérationnelles et n'ont pas de moyens de collecte d'informations. Il revient aux États membres d'assurer le volet opérationnel du renseignement. La SIAC se charge uniquement de l'analyse stratégique.

Cellule de fusion de l'Union européenne contre les menaces hybrides: la communication conjointe sur la lutte contre les menaces hybrides d'avril 2016 désigne la cellule de fusion de l'Union européenne contre les menaces hybrides comme le point focal pour l'analyse des informations provenant de toutes les sources sur les menaces hybrides dans l'Union européenne. Le mandat confié à la cellule a été approuvé en décembre 2016 par la Commission dans le cadre d'une consultation interservices. La cellule de fusion de l'Union européenne contre les menaces hybrides, qui travaille au sein de l'INTCEN, fait partie de la SIAC et collabore dès lors avec l'EUMS INT; un membre militaire permanent est mis à sa disposition. Le terme hybride désigne l'utilisation délibérée par un État ou un acteur non étatique d'une combinaison de plusieurs outils et leviers secrets/publics, militaires/civils, tels que des cyberattaques, des campagnes de désinformation, des activités d'espionnage, des pressions économiques, l'utilisation de forces supplétives, ou autres activités subversives. La cellule de fusion de l'Union européenne contre les menaces hybrides collabore avec un vaste réseau de points de contacts au sein de la Commission et des États membres, afin de fournir la réponse intégrée/l'approche gouvernementale globale requise pour faire face aux différents défis.

SITROOM de l'Union européenne: la salle de veille de l'Union européenne fait partie du Centre d'analyse du renseignement de l'Union européenne (INTCEN) et fournit au SEAE une capacité opérationnelle permettant d'assurer une réaction immédiate et efficace en cas de crises. C'est un organe militaro-civil de veille permanent qui fournit une surveillance et une appréciation de la situation dans le monde entier, 24 heures sur 24 et 7 jours sur 7.

Instruments utiles

Cadre pour une réponse diplomatique conjointe de l'Union européenne face aux actes de cybermalveillance: le cadre, approuvé en juin 2017, fait partie de l'approche de l'Union européenne en matière de cyberdiplomatie, qui contribue à prévenir les conflits, à atténuer les menaces sur la cybersécurité et à offrir une plus grande stabilité dans les relations internationales. Le cadre fait pleinement usage des mesures prises au titre de la politique étrangère et de sécurité commune, y compris, si nécessaire, des mesures restrictives. Le recours aux mesures décidées dans le contexte du cadre devrait encourager la coopération, faciliter la réduction des menaces immédiates et à long terme, et influencer le comportement de l'auteur de la menace ou d'agresseurs potentiels à long terme.

2. COORDINATION DE CRISE DANS LE DOMAINE DE LA CYBERSÉCURITÉ DANS LE DISPOSITIF IPCR — COORDINATION HORIZONTALE ET NIVEAUX D'ACTIVATION POLITIQUE

Le dispositif IPCR peut être (et a été) utilisé pour répondre à des problèmes techniques et opérationnels, mais toujours sous un angle politique/stratégique.

En ce qui concerne les niveaux d'activation, l'IPCR peut être utilisé, en fonction du niveau de crise, en passant du mode «surveillance» au mode «partage d'information», qui est le premier niveau d'activation de l'IPCR, puis au mode «activation intégrale de l'IPCR».

L'activation intégrale du dispositif nécessite une décision de la présidence tournante du Conseil de l'Union européenne. La Commission, le SEAE et le SGC peuvent activer le mode «partage d'information» de l'IPCR. Les modes «surveillance»

et «partage d'information» déclenchent différents niveaux d'échange d'informations, le mode «partage d'information» activant une demande d'élaboration de rapports ISAA. Le mode «activation intégrale» de l'IPCR ajoute à la boîte à outils une table ronde comprenant la présidence (généralement le président du Coreper II ou un expert compétent au niveau des conseillers des représentations permanentes, bien qu'à titre exceptionnel, des tables rondes aient eu lieu au niveau ministériel).

Acteurs

La présidence tournante (habituellement, le président du Coreper) joue le rôle de chef de file.

Pour le Conseil européen, le cabinet du président.

Pour la Commission européenne, niveau secrétaire général adjoint/DG et/ou experts compétents.

Pour le SEAE, niveau secrétaire général adjoint/directeur exécutif et/ou experts compétents.

Pour le SGC, le cabinet du SG, l'équipe de l'IPCR et les DG responsables.

Champ des activités: créer une image commune intégrée de la situation et sensibiliser aux goulets d'étranglement ou aux insuffisances à chacun des trois niveaux afin d'y remédier au niveau politique, ce qui donne lieu à des décisions si elles relèvent de la compétence des participants, ou à des propositions de mesures à soumettre au Coreper II et jusqu'au Conseil.

Appréciation commune de la situation:

(inactif): des pages de surveillance IPCR peuvent être générées pour suivre l'évolution de situations susceptibles de dégénérer en une crise avec des ramifications dans l'Union européenne,

(mode «partage d'information»): des rapports ISAA seront rédigés par le service chef de file sur la base des contributions des services de la Commission, du SEAE et des États membres (par l'intermédiaire des questionnaires IPCR),

(mode «activation intégrale de l'IPCR»): outre les rapports ISAA, des tables rondes informelles IPCR rassemblent différents acteurs concernés des États membres, de la Commission, du SEAE, des agences compétentes, etc. pour examiner les insuffisances et les goulets d'étranglement.

Coopération et réaction

Activer/synchroniser des mécanismes/instruments de gestion de crise supplémentaires, en fonction de la nature et de l'impact de l'incident. Il peut s'agir par exemple du mécanisme de protection civile, du cadre pour une réponse diplomatique conjointe de l'Union européenne face aux actes de cybermalveillance ou du «cadre commun de lutte contre les menaces hybrides».

Communication de crise

Le réseau du communicateur de crise IPCR peut être activé par la présidence, après consultation des services compétents de la Commission, du SGC et du SEAE, afin de soutenir la création de messages communs ou de développer les outils de communication les plus efficaces.

3. GESTION DE CRISE DANS LE DOMAINE DE LA CYBERSÉCURITÉ DANS LE SYSTÈME ARGUS — PARTAGE D'INFORMATION AU SEIN DE LA COMMISSION EUROPÉENNE

Confrontée à des crises imprévues nécessitant une action au niveau européen, telles que les attentats terroristes de Madrid (mars 2004), le tsunami en Asie du Sud-Est (décembre 2004) et les attentats terroristes de Londres (juillet 2005), la Commission a créé, en 2005, le système de coordination ARGUS, soutenu par un système général d'alerte rapide éponyme ([1]) ([2]). Il prévoit un **processus de coordination de crise** spécifique en cas de crise majeure de nature multisectorielle, pour permettre de partager en temps réel des informations liées à la crise et d'assurer une prise de décision rapide.

ARGUS prévoit deux phases en fonction de la gravité de l'événement:

Phase I: est utilisée pour le «partage d'information» sur une crise d'une ampleur limitée

([1]) Commission des Communautés européennes, 23 décembre 2005, communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions: dispositions de la Commission relatives au système d'alerte rapide global «ARGUS», COM(2005) 662 final.

([2]) Décision 2006/25/CE, Euratom.

Exemples d'incidents récemment signalés dans le cadre de la phase I: incendies de forêt au Portugal et en Israël, attentat de Berlin en 2016, inondations en Albanie, ouragan Matthew en Haïti et sécheresse en Bolivie. Chaque DG peut lancer une alerte de phase I lorsqu'elle estime qu'une situation relevant de son domaine de compétence est suffisamment grave pour justifier l'échange d'informations ou en bénéficier. Par exemple, la direction générale des réseaux de communication, du contenu et des technologies ou la direction générale de la migration et des affaires intérieures peut lancer une alerte de phase I lorsqu'elle estime qu'un cyberincident relevant de son domaine de compétence est suffisamment grave pour justifier l'échange d'informations ou en bénéficier.

Phase II: est déclenchée en cas de crise multisectorielle majeure ou de menace prévisible ou imminente pour l'Union

La phase II déclenche une procédure de coordination spécifique permettant à la Commission de prendre des décisions et d'intervenir d'une manière rapide, coordonnée et cohérente, au plus haut niveau, dans son domaine de compétence et en coopération avec les autres institutions. La phase II est déclenchée en cas de crise multisectorielle majeure ou de menace prévisible ou imminente d'une telle crise. Exemples concrets d'événements de phase II: crise des réfugiés/migrants (depuis 2015), triple catastrophe de Fukushima (2011), éruption du volcan Eyjafjallajökull en Islande (2010).

La phase II est activée par le président, de sa propre initiative ou à la demande d'un membre de la Commission. Le président peut attribuer la responsabilité politique de l'intervention de la Commission au commissaire chargé du service le plus concerné par la crise en question, ou décider d'assumer lui-même cette responsabilité.

Il convoque les réunions d'urgence du comité de coordination de crise (CCC). Celles-ci sont organisées sous l'autorité du président ou du commissaire auquel la responsabilité a été attribuée. Elles sont convoquées par le SG au moyen de l'outil informatique ARGUS. Le CCC est une structure opérationnelle particulière de gestion des crises, créée afin de diriger et de coordonner l'intervention de la Commission en cas de crise, qui regroupe les représentants des DG de la Commission, des cabinets et d'autres services de l'Union européenne concernés. Présidé par le secrétaire général adjoint, le **CCC examine la situation, envisage les options, prend des décisions et veille à leur mise en œuvre**, tout en assurant la cohérence de l'intervention. Le SG apporte son soutien au CCC.

4. SYSTÈME DE RÉPONSE AUX CRISES DU SEAE

Le mécanisme de réaction aux crises du SEAE (CRM) est activé à la survenance d'une situation grave ou d'urgence concernant ou impliquant de quelque manière que ce soit la dimension extérieure de l'Union européenne. Le CRM est activé par le secrétaire général adjoint pour la réaction aux crises, après consultation du haut représentant ou du secrétaire général. Le secrétaire général adjoint pour la réaction aux crises peut également être invité à engager le mécanisme de réaction aux crises par le haut représentant, le SG, ou un autre secrétaire général ou directeur exécutif.

Le CRM contribue à la cohérence de l'Union européenne en cas de réaction aux crises dans le cadre de la stratégie de sécurité. En particulier, le CRM facilite les synergies entre les démarches diplomatiques, de sécurité et de défense, et les instruments financiers, commerciaux et de coopération gérés par la Commission.

Le CRM est lié au système général d'alerte rapide de la Commission (ARGUS) et au dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise (IPCR) afin d'exploiter les synergies en cas d'activation simultanée. La salle de veille du SEAE fait office de plateforme de communication entre le SEAE et les systèmes de réaction d'urgence du Conseil et de la Commission.

Normalement, la première action liée à la mise en œuvre du CRM est la convocation d'une **réunion de crise** avec les cadres dirigeants du SEAE, de la Commission et du Conseil directement affectés par la crise en question. Les participants à la réunion évaluent les effets à court terme de la crise et peuvent décider d'adopter des mesures immédiates, d'activer la cellule de crise, ou de convoquer une plateforme de crise. Ces options peuvent être mises en œuvre dans n'importe quel ordre.

La **cellule de crise** est une petite salle d'opérations où les représentants du SEAE, de la Commission et du Conseil intervenant dans les mesures de réaction à la crise se réunissent pour suivre la situation en permanence afin d'apporter un soutien aux décideurs du siège du SEAE. Lorsqu'elle est activée, la cellule de crise est opérationnelle 24 heures sur 24, 7 jours sur 7.

La **plateforme de crise** réunit les services concernés du SEAE, de la Commission et du Conseil afin d'évaluer les effets à moyen et long terme des crises et de s'accorder sur les mesures à prendre. Elle est présidée par le haut représentant, le secrétaire général ou le secrétaire général adjoint chargé de la réponse aux crises. La plateforme de crise évalue l'efficacité de l'action de l'Union européenne dans le pays ou la région, se prononce sur les modifications ou mesures supplémentaires et examine les propositions de mesures à prendre par le Conseil. La plateforme de crise est une réunion ad hoc; par conséquent, elle n'est pas activée en permanence.

La **task force** est composée de représentants des services intervenant dans les mesures de réaction et peut être activée pour suivre et faciliter la mise en œuvre de la réponse de l'Union européenne. Elle évalue l'impact de l'action de l'Union européenne, élabore des documents politiques et des documents d'orientation, contribue à la préparation du cadre politique pour la gestion des crises, contribue à la stratégie de communication et adopte toute autre modalité susceptible de faciliter la mise en œuvre de la réponse de l'Union européenne.

5. DOCUMENTS DE RÉFÉRENCE

On trouvera ci-dessous la liste des documents de référence qui ont été pris en considération lors de l'élaboration du plan d'action:

— *Cadre européen de coopération en cas de crise dans le domaine de la cybersécurité*, version 1, 17 octobre 2012

— *Report on Cyber Crisis Cooperation and Management*, ENISA, 2014

— *Actionable Information for Security Incident Response*, ENISA, 2014

— *Common practices of EU-level crisis management and applicability to cyber crises*, ENISA, 2015

— *Strategies for Incident Response and Cyber Crisis Cooperation*, ENISA, 2016

— *EU Cyber Standard Operating Procedures*, ENISA, 2016

— *A good practice guide of using taxonomies in incident prevention and detection*, ENISA, 2017

— Communication «Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité», COM(2016) 410 final du 5 juillet 2016

— Communication «Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité», conclusions du Conseil (15 novembre 2016), 14540/16

— Décision 2014/415/UE du Conseil du 24 juin 2014 concernant les modalités de mise en œuvre par l'Union de la clause de solidarité (JO L 192 du 1.7.2014, p. 53)

— Achèvement du processus de réexamen du dispositif de coordination dans les situations d'urgence et de crise (CCA): le dispositif intégré de l'Union européenne pour une réaction au niveau politique dans les situations de crise (IPCR), 10708/13, 7 juin 2013

— *Integrated Situational Awareness and Analysis (ISAA) — Standard Operating Procedures*, DS 1570/15, 22 octobre 2015

— Dispositions de la Commission relatives au système d'alerte rapide global «ARGUS», COM(2005) 662 final du 23 décembre 2005

— Décision 2006/25/CE, Euratom de la Commission du 23 décembre 2005 modifiant son règlement intérieur (JO L 19 du 24.1.2006, p. 20)

— *ARGUS Modus Operandi*, Commission européenne, 23 octobre 2013

— Conclusions du Conseil relatives à un cadre pour une réponse diplomatique conjointe de l'Union européenne face aux actes de cybermalveillance («boîte à outils cyberdiplomatique»), document 9916/17

— Protocole opérationnel de l'Union européenne pour la lutte contre les menaces hybrides («EU Playbook»), document SWD(2016) 227

— Mécanisme de réaction aux crises du SEAE, 8 novembre 2016 [Ares(2017)880661]. Document de travail conjoint des services: Protocole opérationnel de l'Union européenne de lutte contre les menaces hybrides («EU Playbook»), SWD(2016) 227 final du 5 juillet 2016

— Communication conjointe au Parlement européen et au Conseil: Cadre commun en matière de lutte contre les menaces hybrides — une réponse de l'Union européenne, JOIN/2016/018 final du 6 avril 2016

— EEAS(2016) 1674 — Document de travail du Service européen pour l'action extérieure — Cellule de fusion de l'Union européenne contre les menaces hybrides — Mandat

6. ÉLÉMENTS SPÉCIFIQUES DE LA CYBERSÉCURITÉ DANS LE PROCESSUS IPCR