

National Cyber Risk Assessment (NCRA) questionnaire: explanatory notes

*Questionnaire d’évaluation nationale du cyberrisque (ENCR) : notes explicatives*

## Context

A National Cyber Risk Assessment (**NCRA**)has been commissioned by the Government of <Country name> to help plan for further investment in cyber security and resilience that may be necessary.

The reason for conducting this National Cyber Risk Assessment is as follows:

* The economic and social development of <Country name> will depend on significant levels of connectivity through cyber space. As in many nations where digitalisation is being introduced on a significant scale, the economy, the administration of government and the provision of essential services will increasingly rely on the integrity of cyberspace and on the infrastructure, systems and data which underpin it. This brings with it opportunities for innovation, growth and efficiency, but is likely to bring risks of societal and economic disruption.
* Introduction of the hardware and software to facilitate this interconnected digital environment has sometimes prioritised efficiency, cost and the convenience of the user, but has not always had security designed in from the start. Malicious actors – hostile states, criminal or terrorist organisations and individuals – can exploit shortcomings. The Government requires assurance that systems being obtained from the commercial market will provide adequate levels of business continuity through cyber security and resilience.

The Government can bring its resources to bear to address cyber threats. But the scale and dynamic nature of cyber threats mean that no Government can directly provide for all aspects of cyber security and resilience. Instead, an approach is needed where industry, infrastructure providers and other partners in the development of <Country name>, collaborate with each other and government in securing networks, services and data. The purpose of this NCRA is therefore

* To provide the Government with a rational basis for prioritizing its own investment in national cyber security
* To assist with the communication of identified risks to key stakeholders to create a culture of cyber risk management, security and resilience.

## Contexte

Une évaluation nationale du cyberrisque (**ENCR**) a été commandée par le Gouvernement du <nom du pays> afin d’aider à la planification des investissements supplémentaires en matière de cybersécurité et de résilience qui pourraient s’avérer nécessaires.

Cette évaluation nationale du cyberrisque est menée aux motifs suivants :

* Le développement économique et social du <nom du pays> dépendra des niveaux de connectivité importants au sein du cyberespace. Comme dans les nombreux pays qui introduisent la digitalisation à grande échelle, l’économie, l’administration du gouvernement et la fourniture de services majeurs dépendront de plus en plus de l’intégrité du cyberespace, ainsi que de l’infrastructure, des systèmes et des données qui le composent. Ce défi s’accompagne d’opportunités d’innovation, de croissance et d’efficacité, mais risque fort d’engendrer des perturbations socio-économiques.
* L’introduction de matériels et de logiciels pour simplifier cet environnement numérique interconnecté a parfois privilégié l’efficacité, les coûts et l’aspect pratique pour l’utilisateur, mais n’a pas toujours intégré dans sa conception un niveau de sécurité adapté. Des acteurs malveillants (États hostiles, individus et organisations criminels ou terroristes) peuvent exploiter les failles. Le gouvernement exige la garantie que les systèmes commercialisés sur le marché offriront les niveaux de continuité opérationnelle appropriés à travers la cybersécurité et la résilience.

Le gouvernement peut mobiliser ses ressources pour lutter contre les cybermenaces. Mais l’ampleur et la nature dynamique des cybermenaces démontrent qu’aucun gouvernement ne peut couvrir directement tous les aspects de la cybersécurité et de la résilience. Il convient plutôt d’adopter une approche collaborative entre l’industrie, les fournisseurs d’infrastructures, d’autres partenaires œuvrant pour le développement du <nom du pays> et le gouvernement pour sécuriser les réseaux, les services et les données. Cette ENCR a donc pour objectif :

* de proposer au gouvernement une base rationnelle pour prioriser ses propres investissements en matière de cybersécurité nationale ;
* de faciliter la communication des risques identifiés aux parties prenantes clés afin de créer une culture de gestion du cyberrisque, de sécurité et de résilience.

## Method

The NCRA will begin with a Survey of significant cyber systems in use by organisations and businesses which use these systems to provide services that are essential for the economy, for Government and for the welfare of the population. These national infrastructure services are by definition.

*“facilities, systems, sites, information, people, networks and processes necessary for <Country name> to function and upon which daily life depends. Typically, these would include: energy, food, water, health, transport, money supply, communications, emergency services and aspects of government including defence. They also include some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (chemical sites for example).”*

The NCRA uses a simplified method of qualitative risk assessment to identify those systems that entail the greatest risk of disruption to these essential services, the economy or society. A ‘screening risk assessment’ - entirely based on the answers given voluntarily by participants in the Survey (you) in response to this Confidential Questionnaire – may be followed by further confidential discussions to enable the Government to evaluate the highest risks.

## Méthode

L’ENCR débutera par une étude des cybersystèmes majeurs utilisés par les organisations ou les entreprises qui exploitent ces systèmes pour fournir des services qui sont essentiels pour l’économie, le gouvernement et le bien-être de la population. Ces services d'infrastructure nationaux sont par définition :

*« Des installations, des systèmes, des sites, des informations, des personnes, des réseaux et des processus nécessaires au bon fonctionnement du <nom du pays> et indispensables au quotidien. En général, ils incluent : l’énergie, l’alimentation, l’eau, la santé, le transport, la masse monétaire, la communication, les services d’urgence et les enjeux gouvernementaux, y compris la défense. Ils intègrent également certaines fonctions, sites et organisations qui ne sont pas indispensables au maintien des services essentiels, mais requièrent une protection en raison du danger potentiel pour le public (sites chimiques par exemple). »*

L’ENCR utilise une méthode simplifiée d’évaluation qualitative des risques pour identifier les systèmes qui comportent le plus grand risque de perturbation pour ces services fondamentaux, l’économie et la société. Une « évaluation préalable des risques », intégralement basée sur les réponses données volontairement par les participants à l’étude (vous) dans le cadre du présent questionnaire confidentiel, peut être suivie par d’autres discussions confidentielles pour permettre au gouvernement d’évaluer les risques les plus sérieux

## The questionnaire

* Answers to the Questionnaire will be confidential: it will be hosted on a [secure government web-site]; [other measures will be taken to protect information]; [detailed answers will not be shared with other participants]
* Participating organisations will be able to contact [the organisers] to clarify questions; and may be asked to meet with [the organisers] to clarify answers they have given
* Feedback will be given on a one-to-one basis to [all] participants in the survey, following the initial or final evaluation phase of the NCRA
* One questionnaire should be answered for every significant cyber-dependent service / system a participating organisation identifies as of interest to the Survey
* The questionnaire is not designed as an audit of cyber security but to inform a qualitative (not quantitative) national-level risk assessment
* The questionnaire uses multiple choices for the main (scoring answers) but allows for short text answers to be given in other cases; please keep answers short and do not include detailed descriptions or technical data.

The Questionnaire will ask you to estimate the nature of the cyber risk in your organisation, in five sections:

* Information about your organisation and critical cyber systems in use
* For each critical cyber/information system you identify:
  + Critical system characteristics of each critical cyber asset
  + Identification of the reasonable worst-case scenario, illustrating the threats and hazards most likely to affect the system
  + The impacts of a successful attack on, or disruption of your critical cyber systems
  + Your estimate of the cyber-security/resilience qualities of your critical cyber-systems

### How cyber risks are calculated

The answers will be used to estimate the cyber risk to <Country name> according to the following formula:

## Le questionnaire

* Les réponses à ce questionnaire seront confidentielles : il sera hébergé sur un [site Web sécurisé du gouvernement] ; [d’autres mesures seront adoptées pour protéger les informations] ; [les réponses détaillées ne seront pas partagées avec les autres participants].
* Les organisations participantes pourront contacter [les organisateurs] pour clarifier les questions et seront peut-être invitées à s’entretenir avec [les organisateurs] afin de clarifier leurs réponses.
* Des commentaires seront fournis de façon individuelle à [tous] les participants à l’étude, après la phase d’évaluation initiale ou finale de l’ENCR.
* Un questionnaire doit être rempli pour chaque service/système cyberdépendant qu’une organisation participante identifie comme intéressant pour l’étude.
* Le questionnaire n’est pas élaboré comme un audit de cybersécurité, mais a pour finalité de renseigner une évaluation qualitative (non quantitative) des risques au plan national.
* Le questionnaire propose des choix multiples pour les principales réponses d’évaluation, mais permet de saisir des réponses courtes dans d‘autres cas. Veuillez fournir des réponses brèves et ne pas inclure de descriptions détaillées ni de données techniques.

Le questionnaire se compose de cinq sections qui vous invitent à évaluer la nature du cyberrisque au sein de votre organisation :

* Informations sur votre organisation et les cybersystèmes stratégiques utilisés
* Pour chaque système d’information/cybersystème :
  + Vous présentez les caractéristiques du système stratégique de chaque ressource informatique capitale.
  + Vous définissez le pire scénario acceptable, illustrant les menaces et les dangers les plus susceptibles d’affecter le système.
  + Vous identifiez les impacts d'une attaque réussie sur vos cybersystèmes stratégiques ou d’une perturbation de vos cybersystèmes stratégiques.
  + Vous évaluez les qualités de cybersécurité/résilience de vos cybersystèmes stratégiques.

### Mode de calcul des cyberrisques

Les réponses seront utilisées pour évaluer les cyberrisques qui pèsent sur le <nom du pays> selon la formule suivante :

## Questionnaire section 1: information about your organisation

**This section will be used to [record information about the organisation, which national infrastructure sector it belongs to, and what services it provides through the use of critical cyber systems.][For confidentiality reasons, the name of the organisation, and the cyber systems identified, will be codified before the information in Sections 2-5 is analysed and compared with information supplied by other participants, so that the collective risk assessment is anonymised]**

In this survey, **Cyber systems** are information systems and networks (hardware, software and associated infrastructure), the data on them, and the services they provide. **Cyber Security** refers to the protection of cyber systems from unauthorised access, harm or misuse. This includes harm caused intentionally by an operator of the system (the ‘insider threat’), or accidentally, as a result of failing to follow security procedures. **‘Cyber resilience’** refers to the ability to prepare for, detect, respond to and recover quickly from cyber-attacks or incidents and so to limit their impact*.*

1.1 Name of the organisation – self-explanatory.

1.2 List the services that your organisations provides: - please describe the range of services provided by the organisation which depend on cyber systems for which you are submitting a Questionnaire response (NB the Survey requires one complete Questionnaire response for each significant cyber system).

1.3 Which national infrastructure Sector does your organisation belong to? – the questionnaire lists the most commonly defined national infrastructure sectors, from which to choose; if none applies, please tick other (and specify which).

1.4 List critical cyber-systems:- list only those cyber-systems in use by your organisation to provide/support provision of services that are critical for the ‘public good’ (public welfare, the economy, essential services); this may be a number of linked systems with similar characteristics, in which case list these as one. Every system you list will need a full questionnaire to be completed – see Q 2.1.

1.5 Cyber security within the organisation – this question concerns the extent to which cyber risks are recognised at Board level (rather than at lower levels, which are covered by Section 5) within the organisation; and whether there is (or not) a Corporate Culture of cyber risk management.

## Questionnaire - section 1 : informations sur votre organisation

**Cette section servira à [enregistrer des informations sur l’organisation, le secteur d'infrastructure national auquel elle appartient et les services qu’elle offre à travers l’utilisation de cybersystèmes stratégiques.] [Pour des raisons de confidentialité, le nom de l’organisation et les cybersystèmes identifiés seront codifiés avant l’analyse des informations des Sections 2-5 et leur comparaison avec les informations fournies par d’autres participants, de sorte que l’évaluation collective des risques soit anonyme.]**

Dans cette étude, **les cybersystèmes** désignent des systèmes d'information et des réseaux (matériels, logiciels et infrastructure associée), les données qu’ils contiennent et les services qu’ils proposent.La **cybersécurité** fait référence à la protection des cybersystèmes contre tout accès non autorisé, acte malveillant ou usage abusif. Cela inclut les actes malveillants commis intentionnellement par un opérateur du système (la « menace interne »), ou accidentellement, suite à l’échec du respect des procédures de sécurité. La **cyberrésilience** désigne la capacité à se préparer à des cyberattaques ou incidents, à les détecter, à y répondre et à s’en relever rapidement, et par conséquent, à limiter leur impact.

1.1 Nom de l’organisation – explicite.

1.2 Liste des services que votre organisation propose : décrivez la gamme des services fournis par l’organisation qui dépendent des cybersystèmes pour lesquels vous répondez au questionnaire (N.B. : l’étude exige une réponse au questionnaire complète pour chaque cybersystème majeur).

1.3 À quel secteur d’infrastructure national votre organisation appartient-elle ? Le questionnaire fournit une sélection des secteurs d'infrastructure nationaux les plus courants ; si aucun ne s’applique, sélectionnez la réponse Autre (et précisez le secteur).

1.4 Donnez la liste des cybersystèmes stratégiques : énumérez uniquement les systèmes utilisés par votre organisation pour fournir/faciliter la fourniture des services qui sont indispensables pour le bien public (bien-être de la population, économie, services essentiels). Il peut s’agir de nombreux systèmes liés présentant des caractéristiques similaires. Dans ce cas, regroupez-les sous une seule réponse. Pour chaque système indiqué, vous devrez remplir un questionnaire complet (voir la question 2.1).

1.5 Cybersécurité au sein de l’organisation : cette question porte sur le niveau de reconnaissance des cyberrisques au niveau de l’exécutif (plutôt qu’à des niveaux inférieurs, qui sont couverts par la Section 5) au sein de l’organisation ; et sur l’existence ou non d’une culture d’entreprise pour la gestion des cyberrisques.

## Questionnaire section 2: critical system characteristics

**This section focuses on one of your critical systems and captures the characteristics and functions of the system.**

2.1. Which of the cyber systems at 1.4 does this questionnaire describe? Which department, organisation or business is responsible for this system? Each questionnaire response should only describe one cyber-system; if your organisation has identified more than one in response to Section 1, then you should identify which system this questionnaire refers to, and which department or part of your organisation is responsible for it.

2.2 Brief description of the system:- please describe the system and its functions briefly – technical details are not required.

2.3 Indicate briefly why this system has been identified by you as a significant system providing or supporting the provision of services that are essential for <Country name> to function.

2.4 System connectivity – a significant element of the risk presented by cyber systems is the extent to which they are insulated from other systems or networks, and the extent to which ‘firewalls’ can become eroded over time; please consider whether your system is truly stand-alone or has become partly linked to other networks in use within or outside the organisation. Also consider the extent to which the system controls physical outcomes (as do, for example, SCADA systems, the ‘Internet of Things’) which affect daily life.

2.5 System hosting – self-explanatory

2.6 & 2.7. Responsibility for cyber security – if the system is not hosted on IT that is owned and managed by your organisation (see 2.3) then responsibility for security may be divided between your organisation and an external provider. In that case, please tick ‘No’ and explain in 2.7.

2.8 Internal business criticality - answers to this question should take account of the extent to which there is effective back-up/redundancy in your system, enabling the effects of disruption to be mitigated; if there is any doubt about the effectiveness of back-up systems (e.g. because they may be exposed to the same risk as the primary system) then the marking should reflect this.

2.9 External business criticality – this question considers only how many people and organisations depend on the service that you are providing, using the cyber system identified at 2.1, for their welfare, livelihood or businesses.

2.11 Outward dependencies: this question is specifically asking about cyber-dependencies – direct reliance on cyber-systems (e.g. the Internet) which are operated by other organisations. Do not include dependence on non-cyber-services provided by others (e.g. electricity supply) even if you believe they are likely to rely on cyber-space

2.12 Inward dependencies: this question asks whether other systems operated by other organisations directly depend on the cyber-system covered by this questionnaire.

## Questionnaire - section 2 : caractéristiques des systèmes stratégiques

**Cette section est centrée sur l’un de vos systèmes stratégiques et collecte les caractéristiques et les fonctions du système.**

2.1. Lequel des cybersystèmes énoncés à la section 1.4 est décrit dans ce questionnaire ? Quel service, quelle organisation ou quelle activité est responsable de ce système ? Chaque réponse du questionnaire ne doit décrire qu’un seul cybersystème. Si votre organisation a identifié plusieurs systèmes dans sa réponse à la Section 1, alors vous devez préciser le système auquel ce questionnaire se réfère et le service ou la partie de l’organisation qui en a la responsabilité.

2.2 Description brève du système : décrivez brièvement le système et ses fonctions. Les détails techniques ne sont pas nécessaires.

2.3 Indiquez brièvement pourquoi vous avez identifié ce système comme étant un système important fournissant ou facilitant la fourniture de services essentiels au fonctionnement du <nom du pays>.

2.4 Connectivité du système : un élément significatif du risque lié aux cybersystèmes est leur degré d’isolement vis-à-vis des autres systèmes ou réseaux, et le niveau de dégradation des « pare-feu » dans le temps. Demandez-vous si votre système est vraiment autonome ou s’il est partiellement lié à d’autres réseaux utilisés au sein ou en dehors de l’organisation. Demandez-vous également dans quelle mesure le système contrôle les répercussions physiques (comme le font, par exemple, les systèmes SCADA, l’Internet des objets ») qui affectent le quotidien.

2.5 Hébergement du système : explicite

2.6 et 2.7. Responsabilité de la cybersécurité : si le système n’est pas hébergé sur une plate-forme informatique détenue et gérée par votre organisation (voir 2.3), alors la responsabilité de la sécurité peut être partagée entre votre organisation et un fournisseur externe. Dans ce cas, sélectionnez « Non » et donnez une explication dans la section 2.7.

2.8 Sensibilité de l’activité interne : les réponses à cette question doivent prendre en compte le degré d’efficacité de la sauvegarde/redondance dans votre système permettant d’atténuer les effets de la perturbation. En cas de doute sur l’efficacité des systèmes de sauvegarde (par exemple, parce qu’ils sont exposés au même risque que le système principal), la sélection doit refléter cet aspect.

2.9 Sensibilité de l’activité externe : cette question prend uniquement en compte le nombre de personnes et d’organisations qui dépendent du service que vous fournissez à l’aide du cybersystème identifié à la section 2.1, pour leur bien-être, leurs moyens de subsistance ou leurs activités.

2.11 Dépendances externes : cette question porte spécifiquement sur les cyberdépendances, c’est-à-dire l’appui direct sur les cybersystèmes (par exemple, Internet) qui sont exécutés par d’autres organisations. N’incluez pas la dépendance vis-à-vis des services non informatiques fournis par d’autres (par exemple, la fourniture d’électricité) même si vous pensez qu’ils sont susceptibles de dépendre d’un cyberespace.

2.12 Dépendances internes : cette question permet de savoir si d’autres systèmes exécutés par d’autres organisations dépendent directement du cybersystème traité dans ce questionnaire.

## Questionnaire section 3: cyber risks

**This section is to identify the cyber risk, and to determine what would be a ‘reasonable worst-case scenario’ illustrating the risks to your system. The cyber risk is an event that affects objects of value (property, business continuity, profitability, etc.) to your organisation. The Survey identifies the risk by inviting you to construct a scenario representing the worst that could reasonably happen to your system given its function, the kinds of ‘threat actors’ who are known to be motivated to attack such systems, and the methods (‘threat vectors’) they have to do so.**

**See Annex A for extracts from the UK’s National Cyber Security Strategy describing the different kinds of threat actor and attack vector (methodology) and giving examples that may help to answer questions in this section.**

3.1 The three aspects of information security – this question asks you which of the following aspects is the most important to the system you have described in this questionnaire response. The definitions of the three aspects is as follows:

|  |  |
| --- | --- |
| Availability | information can be accessed by the user when it is needed |
| Integrity | information has not been changed accidentally, or deliberately, and is accurate and complete |
| Confidentiality | information is only available to those who have a right to know it |

The definitions of the scores used to assess the importance of the tree aspects of information security to your organisation is as follows:

|  |  |
| --- | --- |
| Low | This aspect of information security is not significant for the delivery of essential services and any disruption to system operation, loss of integrity or breach of confidential information will have little impact on the delivery of services or the reputation of the organisation. |
| Medium | This aspect of information security is important to the successful delivery of some services and any disruption to system operation, loss of integrity or breach of confidential information will have a limited and manageable impact of some key services and the reputation of the organisation. |
| High | This aspect of information security is very important to the successful delivery of essential services and any disruption to system operation, loss of integrity or breach of confidential information will have a severe impact on some key services and the reputation of the organisation |
| Very High | This aspect of information security is critical to the successful delivery of essential services and any disruption to system operation, loss of integrity or breach of confidential information will have a severe, widespread and long-term impact on key services and the reputation of the organisation |

## Questionnaire - section 3 : cyberrisques

**Cette section vise à identifier le cyberrisque et à déterminer le « pire scénario acceptable » illustrant les risques encourus par votre système. Le cyberrisque est un événement qui affecte les objets de valeur (propriété, continuité de service, rentabilité, etc.) de votre organisation. L’étude identifie d’abord le risque en vous invitant à élaborer un scénario représentant la pire situation qui pourrait raisonnablement se produire pour votre système compte tenu de sa fonction, puis les types « d’auteurs de menaces » dont les motivations connues sont l’attaque de ces systèmes, et enfin les méthodes (« vecteurs de menaces ») qu’ils utilisent pour y parvenir.**

**Consultez l’Annexe A pour lire des extraits de la Stratégie nationale de cybersécurité du Royaume-Uni qui décrit les différents types d’auteurs de menaces et vecteurs d’attaques (méthodologie), et fournit des exemples utiles pour répondre aux questions de cette section.**

3.1 Les trois aspects de la sécurité de l’information : dans cette question, il vous est demandé lesquels des aspects suivants sont les plus importants pour le système que vous avez décrit dans votre réponse à ce questionnaire. Ces trois aspects sont définis comme suit :

|  |  |
| --- | --- |
| Disponibilité | L’utilisateur peut accéder aux informations quand il en a besoin. |
| Intégrité | Les informations n’ont pas été modifiées accidentellement ou délibérément, elles sont précises et complètes. |
| Confidentialité | Les informations sont uniquement disponibles pour ceux qui ont le droit d’en connaître. |

Les notes utilisées pour évaluer l’importance des trois aspects de la sécurité de l’information pour votre organisation sont définies comme suit :

|  |  |
| --- | --- |
| Faible | Cet aspect de la sécurité de l’information n’est pas important pour la fourniture de services essentiels et toute perturbation du fonctionnement du système, perte d'intégrité ou fuite des informations confidentielles aura un faible impact sur la fourniture des services ou la réputation de l’organisation. |
| Moyen | Cet aspect de la sécurité de l’information est important pour la fourniture de certains services et toute perturbation du fonctionnement du système, perte d'intégrité ou fuite des informations confidentielles aura un impact limité et gérable sur la fourniture de certains services majeurs et la réputation de l’organisation. |
| Élevé | Cet aspect de la sécurité de l’information est très important pour la fourniture de services essentiels et toute perturbation du fonctionnement du système, perte d'intégrité ou fuite des informations confidentielles aura un impact sérieux sur la fourniture de certains services majeurs et la réputation de l’organisation. |
| Très élevé | Cet aspect de la sécurité de l’information est primordial pour la fourniture de services essentiels et toute perturbation du fonctionnement du système, perte d'intégrité ou fuite des informations confidentielles aura un impact sérieux, étendu et durable sur la fourniture de certains services majeurs et la réputation de l’organisation. |

3.2 Importance of cyber threat intelligence – Organisations whose cyber-systems are exposed to the threat of attack rely on up-to-date information about threat actors and threat methodologies to ensure that their systems remain secure, and to trigger effective incident response. These questions ask you how readily you are able to obtain up-to-date cyber threat information and how important you think it is to the security of the system that you are assessing. The definition of the scores used to assess the importance of threat intelligence to your organisation is as follows:

|  |  |
| --- | --- |
| 1 | Threat intelligence is not used as part of the organisations approach to cyber security |
| 2 | Threat intelligence is occasionally made available but is not an important aspect of the approach to cyber security |
| 3 | Threat intelligence is sometimes sought and used on an ad-hoc basis to improve cyber security |
| 4 | Threat intelligence is an important part of the approach to cyber security and a process is in place to ensure that appropriate action is taken to respond to new or changing threats. |
| 5 | Threat intelligence is an essential part of the approach to cyber security and is used to provide timely response to changes in the cyber security threat environment |

3.4 The ability of your organisation to access threat intelligence is assessed as follows:

|  |  |
| --- | --- |
| 1 | Threat intelligence is not available |
| 2 | Threat intelligence is occasionally made available on an ad-hoc basis |
| 3 | At least one source of relevant threat intelligence is accessed on a regular basis (e.g. monthly) |
| 4 | Several high-quality threat intelligence feeds are actively and frequently gathered and analysed (e.g. daily) |
| 5 | Multiple (all source) feeds of high-quality threat intelligence are actively gathered, analysed and used to provide a tailored near real time insight into the cyber security threat environment. |

3.2 Importance des renseignements sur les cybermenaces : les organisations dont les cybersystèmes sont exposés à la menace d’une attaque s’appuient sur des informations actualisées sur les auteurs et les méthodologies des menaces afin de garantir la sécurité de leurs systèmes et déclencher une réponse efficace à la suite d’un incident. Dans ces questions, il vous est demandé d’estimer votre niveau de préparation pour obtenir des informations actualisées sur les cybermenaces et le degré d’importance de ces informations pour la sécurité du système que vous évaluez. Les notes utilisées pour évaluer l’importance des renseignements sur les menaces pour votre organisation sont définies comme suit :

|  |  |
| --- | --- |
| 1 | Les renseignements sur les menaces ne sont pas utilisés dans l’approche de cybersécurité des organisations. |
| 2 | Les renseignements sur les menaces sont disponibles de façon occasionnelle, mais ne constituent pas un aspect important de l’approche de cybersécurité. |
| 3 | Les renseignements sur les menaces sont parfois recherchés et exploités de manière ad hoc pour améliorer la cybersécurité. |
| 4 | Les renseignements sur les menaces sont un aspect important de l’approche de cybersécurité et un processus est en place pour garantir que des mesures adaptées sont mises en œuvre pour contrer des menaces nouvelles ou évolutives. |
| 5 | Les renseignements sur les menaces sont un volet essentiel de l’approche de cybersécurité et sont exploités pour fournir une réponse rapide aux changements de l’environnement des menaces de la cybersécurité. |

3.4 La capacité de votre organisation à accéder aux renseignements sur les menaces est évaluée de la façon suivante :

|  |  |
| --- | --- |
| 1 | Les renseignements sur les menaces ne sont pas disponibles. |
| 2 | Les renseignements sur les menaces sont accessibles de façon occasionnelle et ad hoc. |
| 3 | Au moins une source de renseignements pertinents sur les menaces est accessible de façon régulière (par exemple, chaque mois). |
| 4 | Plusieurs flux de renseignements de haute qualité sur les menaces sont regroupés et analysés de façon active et régulière (par exemple, chaque jour). |
| 5 | Plusieurs flux (toutes sources confondues) de renseignements de haute qualité sur les menaces sont regroupés, analysés et exploités pour fournir des informations personnalisées quasiment en temps réel sur l’environnement des menaces de la cybersécurité. |

3.5 – 3.6 Which cyber **threat actors** are you most concerned about? Which cyber-**attack vectors** are you most concerned about? This question concerns only the cyber system being assessed: taking into consideration the relative importance of (see Question 3.1) availability, integrity, and confidentiality of the data on your system, which kind of threat actor (criminal, state/state-sponsored, hacktivist, terrorist) is most likely to be motivated and able to attack the system successfully; and which attack methodology would be of most concern to you. For some organisations/systems, accidental disruption is as big a concern as any malicious threat actor.

|  |  |
| --- | --- |
| **Threat Actor** | **Commonly associated threat vectors** |
| **Cyber criminals** | Cyber-**dependent** crimes (e.g. developing and propagating malware for financial gain, hacking to steal, damage distort or destroy data, networks; includes ransomware and threats of distributed denial of service – DDOS – for extortion |
| Cyber-**enabled** crimes – traditional crimes increased in scale by use of computers, networks or other forms of ICT (e.g. cyber-enabled fraud and data theft) |
| **States and State-sponsored threat (generally covert)** | Embarrassing outages of communications, IT and networked services etc |
| Espionage |
| Offensive cyber capabilities including destructive capabilities threatening security of CNI, industrial control systems, the ‘Internet of Things’, etc |
| **Terrorists** | Hitherto low technical capability, including defacements, ‘doxing’ (where hacked personal details are ‘leaked’ online) designed to attract media attention and intimidate victims |
| Future threat may increase as an increasingly computer-literate generation exploits possibilities of defacement or DDOS activity against States |
| **Hacktivists, insiders and others** | Disruptive activity (website defacement; DDOS) and some more lasting damage by individuals with a grievance |
| Insider threat: theft of sensitive data and intellectual property; possible destructive DDOS |
| **Accidental** | Accidental damage by employees’ inadvertent infection of networked systems |

3.7 Reasonable worst-case scenario: you are asked to use your ‘top’ answers to 3.1, 3.5 and 3.6 to construct a scenario, as follows:

“*The reasonable worst-case scenario for this system is a successful attack by [top answer to 3.5] using [top answer to 3.6] resulting in a significant breach of [top answer to 3.1]”*

3.5 – 3.6 Par quels **auteurs de cybermenaces** êtes-vous le plus concerné ? Par quels **vecteurs de cyberattaques** êtes-vous le plus concerné ? Cette question porte uniquement sur le cybersystème en cours d’évaluation : en prenant en compte l’importance relative (voir question 3.1) de la disponibilité, de l’intégrité et de la confidentialité des données sur votre système, indiquez quel type d’auteur de menace (criminel, État/menace parrainée par l’État, hacktiviste, terroriste) est le plus susceptible de vouloir et de pouvoir mener à bien une attaque sur le système, et quelle méthodologie d’attaque serait la plus préoccupante selon vous. Pour certains systèmes/organisations, une perturbation accidentelle est aussi préoccupante qu'un auteur de menace malveillant.

|  |  |
| --- | --- |
| **Auteur de menace** | **Vecteurs de menaces couramment associés** |
| **Cybercriminels** | Les crimes **cyberdépendants** (par exemple, le développement et la propagation de logiciels malveillants par appât du gain, le piratage pour voler, dégrader, déformer ou détruire des données ou des réseaux) incluent les ransomware et les menaces de déni de service distribué (DDOS) pour extorsion. |
| Les **cybercrimes** désignent les crimes traditionnels qui se sont développés à grande échelle du fait de l’utilisation des ordinateurs, réseaux ou autres formes de TIC. Par exemple, fraude informatique et vol de données. |
| **Menace émanant des États et parrainée par les États (généralement masqués)** | Coupures gênantes des communications, des services informatiques et en réseau, etc. |
| Espionnage |
| Cybercapacités offensives incluant des capacités destructrices menaçant la sécurité des infrastructures nationales critiques (CNI), des systèmes de contrôle industriels, l’Internet des objets, etc. |
| **Terroristes** | Jusqu’à présent, activités de faible capacité technique, incluant des dégradations, le « doxing » (diffusion en ligne de données personnelles piratées), conçues pour attirer l’attention des médias et intimider les victimes. |
| La menace future peut s’intensifier, car une nouvelle génération de terroristes bien formés à l'informatique exploite les possibilités de dégradation ou d’activité DDOS contre les États. |
| **Hacktivistes, menaces internes et autres** | Perturbations (dégradation de site Internet, DDOS) et certains dommages plus durables commis par des individus ayant des griefs. |
| Menace interne : vol de données sensibles et de propriété intellectuelle ; activité DDOS potentiellement destructrice |
| **Accidents** | Dommage accidentel causé par des employés qui se traduit par l’infection involontaire des systèmes en réseau |

3.7 Pire scénario acceptable : il vous est demandé d’utiliser vos « meilleures » réponses aux questions 3.1, 3.5 et 3.6 pour élaborer un scénario, par exemple :

*« Le pire scénario acceptable pour ce système est une attaque réussie par [meilleure réponse à la question 3.5] utilisant [meilleure réponse à la question 3.6] et donnant lieu à une fuite importante de [meilleure réponse à la question 3.1]. »*

## Questionnaire section 4: impacts

**This Section asks you to estimate the scale of impact in the event of an attack according to the reasonable worst-case scenario. Assume for the purposes of this Survey that the attack is successful, even if you consider that this is unlikely (the likelihood of a successful attack will be part of the assessment following completion of Section 5). You may find it useful to consider the case histories attached to this note which provide examples of organisations worldwide who have been successfully attacked.**

**Impacts are measured taking into account how widespread, how intense, and how long-lasting they are likely to be; the overall impact is taken into account. If the impact in one area is negligible, please use the ‘no impact’ column.**

4.1 Impact on people who use your services – the measure here is how many **people** who rely on your services would be affected by a successful attack.

4.2 Impact on other essential services – this question is trying to find out how many **other** essential services would be affected by a disruption to your cyber system. If the answer is that there are no knock-on consequences for other organisations in the national infrastructure sectors, then please mark ‘no impact’ against each.

* A ‘low impact’ is one where any impact is likely to be limited, localised in one area, and of short duration (minutes rather than hours).
* A ‘medium impact’ would be more intense, not localised but not nationwide, and of longer duration (hours).
* A ‘high impact’ would involve very significant and widespread disruption to the service, for a sustained period of time (days).

Case Study 3 (the 2013 Power Grid Attack in Ukraine) provides an example of a cyber-attack that does not only affect direct customers of an organisation that is attacked, but also has indirect knock-on effects on a wider customer base through other national infrastructure owners.

## Questionnaire - section 4 : impacts

**Cette section vous demande d’évaluer le niveau d’impact en cas d’attaque dans le pire scénario acceptable. Imaginons pour les besoins de cette étude que l’attaque réussisse, même si vous pensez que cela est improbable (la probabilité d’une attaque réussie sera traitée dans l’évaluation une fois la section 5 complétée). Les études de cas jointes à cette note fournissent des exemples d’organisations internationales ayant fait l’objet d’une attaque et pourraient vous être utiles.**

**Les impacts sont mesurés en tenant compte de l’étendue, de l’intensité et de la durée potentielles de ces attaques. L’impact général est pris en compte. Si l’impact dans un domaine est négligeable, utilisez la colonne « Aucun impact ».**

4.1 Impact sur les personnes utilisant vos services : on mesure ici le nombre de **personnes** dépendantes de vos services qui seraient touchées par une attaque réussie.

4.2 Impact sur d’autres services essentiels : cette question tente de déterminer combien d’autres services essentiels seraient affectés par une perturbation de votre cybersystème. Si la réponse est qu’il n’existe aucune conséquence indirecte pour les autres organisations des secteurs d’infrastructure nationaux, alors indiquez « Aucun impact » pour chacun d’entre eux.

* Un « impact faible » désigne un impact probablement limité, localisé dans une zone et de courte durée (minutes plutôt qu’heures).
* Un « impact moyen » serait plus intense, non localisé, mais pas national, et de plus longue durée (heures).
* Un « impact élevé » impliquerait une perturbation du service très importante et étendue pendant une longue période (jours).

L’étude de cas 3 (attaque du réseau électrique ukrainien en 2013) fournit l’exemple d’une cyberattaque qui n’affecte pas uniquement les clients directs d’une organisation faisant l’objet de l’attaque, mais a aussi des effets indirects sur une base de clients élargie par le biais d’autres exploitants d’infrastructures nationales.

4.3 Estimate the impact on industry and the economy. As can be seen from the case studies at Annex A, the financial damage can easily get into the Millions. The scale used for this NCRA is accordingly (using GDP of 20 000 000M XAF)

|  |  |  |
| --- | --- | --- |
| **Scale** | **%age of GDP** | **$ equivalent [adjust for the size of the economy] or adopt the following figures specific to <Country name>** |
| Low | Less the 0.001% | Less than 200M XAF |
| Medium | 0.001-0.005% | 201M-1000M XAF |
| High | 0.005-0.025% | 1001M-5000M XAF |
| Very High | More than 0.025% | More than 5000M XAF |

4.4 Estimate the impact on [non-material ‘objects of value’ to <Country name>]. The judgements here will be subjective, but you are invited to consider three dimensions of each impact type:

* Intensity - is the impact highly intensive or less so, on a scale from 1-3
* Extent – is the impact localised, or widespread (nationwide), on a scale from 1-3
* Duration – is the impact short-lived (days), or long-lived (months), on a scale from 1-3

Combining the scores will give you an overall impact score of low (3-4), medium (5-6), or high (7-9)

4.3 Estimez l’impact sur le secteur et l’économie. Comme l’illustrent les études de cas de l’Annexe A, les dommages financiers peuvent facilement atteindre millions. L’échelle utilisée pour cette ENCR est adaptée en conséquence. (PIB = 20 000 000M XAF)

|  |  |  |
| --- | --- | --- |
| **Échelle** | **Pourcentage du PIB** | **Équivalent en dollars [modifiez l'échelle de valeurs] ou adoptez les chiffres suivants propres au <nom du pays>** |
| Faible | Inférieur à 0,001 % | Inférieur à 200M XAF |
| Moyen | 0,001-0,005 % | 201M-1000M XAF |
| Élevé | 0,005-0,025 % | 1001M-5000M XAF |
| Très élevé | Supérieur à 0,025 % | Supérieur à 5000M XAF |

4.4 Estimez l’impact sur des [« objets de valeur » non matériels pour le <nom du pays>]. Les jugements ici sont subjectifs, mais vous êtes invité à examiner les trois dimensions de chaque type d’impact :

* Intensité : impact plus ou moins élevé, sur une échelle de 1 à 3
* Ampleur : impact localisé ou étendu (au plan national), sur une échelle de 1 à 3
* Durée : impact de courte durée (jours) ou de longue durée (mois), sur une échelle de 1 à 3

La combinaison des scores vous donnera un niveau d’impact général faible (3-4), moyen (5-6) ou élevé (7-9).

## Questionnaire section 5: system vulnerabilities

You are invited to self-assess the vulnerability of your cyber systems using a simplified approach, based on the UK National Cyber Security Centre’s ’10 steps to cyber security’, which recommends a regime based on the 10 steps listed below:

**UK National Cyber Security Centre: 10 Steps to Cyber Security**

**1. Risk Management Regime.** Embed an appropriate risk management regime across the organisation. This should be supported by an empowered governance structure, which is actively supported by the board and senior managers. Clearly communicate your approach to risk management with the development of applicable policies and practices. These should aim to ensure that all employees, contractors and suppliers are aware of the approach, how decisions are made, and any applicable risk boundaries.

**2. Secure configuration.** Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

**3. Network security.** The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

**4. Managing user privileges.** If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as ‘least privilege’.

**5. User education and awareness.** Users have a critical role to play in their organisation’s security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.

## Questionnaire - section 5 : vulnérabilités du système

Vous êtes invité à auto-évaluer la vulnérabilité de votre cybersystème en utilisant une approche simplifiée, fondée sur les dix mesures élaborées par le Centre national de cybersécurité du Royaume-Uni, qui recommande un régime basé sur les 10 mesures énoncées ci-après :

**Centre national de cybersécurité du Royaume-Uni : 10 mesures de cybersécurité**

**1. Régime de gestion des risques.** Intégrez un régime de gestion des risques approprié au sein de l’organisation. Ce régime peut être soutenu par une structure de gouvernance habilitée, qui est soutenue activement par le comité exécutif et les hauts dirigeants. Communiquez clairement votre approche de la gestion des risques à travers le développement de politiques et de pratiques applicables. Leur objectif est de garantir que tous les employés, prestataires et fournisseurs sont informés de l’approche, du processus décisionnel et des limites des risques applicables.

**2. Configuration sécurisée.** La conception d’une approche pour identifier les versions et

processus technologiques de base visant à gérer la configuration peut fortement améliorer la sécurité des systèmes. Vous devez élaborer une stratégie pour supprimer ou désactiver les fonctionnalités inutiles de vos systèmes et éliminer rapidement les vulnérabilités connues, généralement à l’aide de correctifs. Si vous ne le faites pas, vous risquez fortement de compromettre les systèmes et les informations.

**3. Sécurité des réseaux.** Les connexions de vos réseaux à Internet et à d’autres réseaux de partenaires exposent vos systèmes et technologies aux attaques. En créant et en instaurant certaines politiques simples et des solutions techniques et architecturales adaptées, vous pouvez réduire les chances de réussite de ces attaques (ou de nuisance pour votre organisation). Les réseaux de votre organisation couvrent certainement de nombreux sites et le recours au travail mobile ou à distance, ainsi qu’aux services Cloud, complexifie la définition de limites de réseau fixes. Plutôt que de vous concentrer exclusivement sur les connexions physiques, pensez aux emplacements de stockage et de traitement de vos données, ainsi qu’aux sites où un assaillant aurait l’opportunité d’interférer avec vos données.

**4. Gestion des privilèges des utilisateurs.** Si les utilisateurs disposent de privilèges système ou de droits d’accès inutiles, alors l’impact d’un usage abusif ou d’une compromission de ces comptes utilisateurs sera plus grave que nécessaire. Tous les utilisateurs doivent bénéficier du niveau de privilèges et de droits système raisonnable (mais minimal) nécessaire pour leur rôle. L’octroi de privilèges système très élevés doit faire l’objet d’une gestion et d’un contrôle rigoureux. Ce principe est parfois appelé « moindre privilège ».

**5. Éducation et sensibilisation des utilisateurs.** Les utilisateurs ont un rôle essentiel à jouer dans la sécurité de leur organisation et il est donc important que les règles de sécurité et les technologies fournies permettent aux utilisateurs de remplir leur mission tout en préservant la sécurité de l’organisation. Ce principe peut systématiquement s’accompagner de programmes et de formations de sensibilisation offrant une expertise de sécurité et favorisant l'instauration d’une culture de la sécurité.

**6. Incident management.** All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise.

**7. Malware prevention.** Malicious software, or malware is an over-arching term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.

**8. Monitoring.** System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

**9. Removable media controls.** Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

**10. Home and mobile working.** Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. You should establish risk-based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.

**6. Gestion des incidents.** Toutes les organisations seront confrontées à des incidents de sécurité à un moment donné. L’investissement dans la mise en place de politiques et de processus de gestion efficace des incidents permettra d’améliorer la résilience, de soutenir la continuité de l’activité, de renforcer la confiance des clients et des parties prenantes, et potentiellement de réduire les impacts. Vous devez identifier des sources (internes et externes) reconnues d’expertise de gestion des incidents.

**7. Prévention contre les logiciels malveillants.** Un logiciel malveillant est un terme général pour désigner tout code ou contenu pouvant avoir un impact nuisible et indésirable sur des systèmes. Tout échange d’informations présente le risque que des logiciels malveillants circulent, ce qui pourrait avoir de graves conséquences sur vos systèmes et vos services. Le risque peut être réduit en concevant et en mettant en œuvre des politiques de lutte contre les logiciels malveillants adaptées dans le cadre d’une approche générale profondément axée sur la défense.

**8. Surveillance.** La surveillance des systèmes permet de détecter des attaques réelles ou des tentatives d’attaque sur des systèmes ou des services de l’entreprise. Une bonne surveillance est essentielle pour contrer efficacement les attaques. De plus, la surveillance vous offre la garantie que les systèmes sont utilisés de façon appropriée conformément aux politiques de l’organisation. La surveillance est souvent une capacité clé indispensable pour respecter les exigences légales et réglementaires.

**9. Contrôles des supports amovibles.** Les supports amovibles représentent un moyen courant d’introduire des logiciels malveillants et d’exporter accidentellement ou délibérément des données sensibles. Vous devez définir clairement votre besoin professionnel d’utilisation de supports amovibles et appliquer les contrôles de sécurité appropriés pour cet usage.

**10. Télétravail et travail mobile.** L’accès au travail mobile et aux systèmes à distance offre de sérieux avantages, mais expose à de nouveaux risques qui doivent être gérés. Vous devez mettre en place des politiques et des procédures basées sur les risques qui facilitent le travail mobile ou l’accès distant aux systèmes et s’appliquent aux utilisateurs et aux prestataires de services. Formez les utilisateurs à se servir de leurs appareils mobiles en toute sécurité dans leurs environnements professionnels potentiels.

## Annex A: cyber threats and hazards

**(Extract from the UK’s National Cyber Security Strategy, Chapter 3)**

**Cyber criminals**

This strategy deals with cyber-crime in the context of two interrelated forms of criminal activity:

**•** cyber-dependent crimes – crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data)

**•** cyber-enabled crimes – traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

Much of the most serious cyber-crime – mainly fraud, theft and extortion – against the UK continues to be perpetrated predominantly by financially motivated Russian-language Organised Criminal Groups (OCGs) in Eastern Europe, with many of the criminal marketplace services being hosted in these countries. However, the threat also emanates from other countries and regions, and from inside the UK itself, with emerging threats from South Asia and West Africa of increasing concern.

Even when the main individuals responsible for the most damaging cyber-criminal activities against the UK are identified, it is often difficult for the UK and international law enforcement agencies to prosecute them when they are located in jurisdictions with limited, or no, extradition arrangements.

These OCGs are principally responsible for developing and deploying the increasingly advanced malware that infects the computers and networks of UK citizens, our industry and government. The impact is dispersed throughout the UK, but the cumulative effect is significant. These attacks are becoming increasingly aggressive and confrontational, as illustrated by the increasing use of ransomware, and threats of distributed denial of service (DDoS) for extortion.

Whilst OCGs may pose a significant threat to our collective prosperity and security, equally of concern is the continuing threat from acts of less sophisticated but widespread cybercrimes carried out against individuals or smaller organisations.

## Annexe A : Cybermenaces et dangers

**(Extrait de la Stratégie nationale de cybersécurité du Royaume-Uni, Chapitre 3)**

**Cybercriminels**

Cette stratégie aborde la cybercriminalité dans le contexte de deux formes d’activités criminelles interdépendantes :

**•** Crimes cyberdépendants : crimes pouvant être commis uniquement à l’aide de dispositifs TIC (Technologies de l’information et de la communication) qui constituent à la fois l’outil utilisé pour commettre le crime et l’objet du crime (par exemple, développement et propagation de logiciels malveillants par appât du gain, piratage pour voler, dégrader, déformer ou détruire des données).

**•** Cybercrimes : crimes traditionnels pouvant se multiplier à grande échelle ou ampleur en utilisant des ordinateurs, réseaux informatiques ou autres formes de TIC. Par exemple, fraude informatique et vol de données.

Une grande partie de la cybercriminalité la plus grave (principalement la fraude, le vol et l’extorsion) qui menace le Royaume-Uni continue d’être initiée, de façon prédominante, par des acteurs du crime organisé d’Europe de l’Est qui parlent russe et affichent des motivations financières. De nombreux services sur le marché du crime sont hébergés dans ces pays. Cependant, la menace émane également d’autres pays et régions, et au sein même du Royaume-Uni, à travers des menaces émergentes de plus en plus préoccupantes venues d’Asie du Sud et d’Afrique de l’Ouest.

Même lorsque les principaux responsables des activités cybercriminelles les plus nuisibles perpétrées contre le Royaume-Uni sont identifiés, il est souvent difficile pour le Royaume-Uni et les forces de l’ordre internationales de les poursuivre lorsqu’ils se trouvent dans des juridictions avec des accords d’extradition limités ou inexistants.

Ces acteurs du crime organisé sont principalement responsables du développement et du déploiement de logiciels malveillants de plus en plus sophistiqués qui infectent les ordinateurs et les réseaux des citoyens britanniques, de notre secteur et du gouvernement. Les répercussions sont disséminées dans l’ensemble du Royaume-Uni, mais l’effet cumulé est important. Ces attaques deviennent de plus en plus agressives et conflictuelles comme l’illustre l’utilisation croissante des ransomware et des menaces de déni de service distribué (DDOS) pour extorsion.

Alors que les acteurs du crime organisé peuvent constituer une menace de taille pour notre prospérité et sécurité collective, la menace permanente d’actes cybercriminels moins sophistiqués, mais étendus, perpétrés à l’encontre des personnes ou d’organisations plus petites, est tout aussi préoccupante.

**States and state-sponsored threats**

We regularly see attempts by states and state-sponsored groups to penetrate UK networks for political, diplomatic, technological, commercial and strategic advantage, with a principal focus on the government, defence, finance, energy and telecommunications sectors.

The capacity and impact of these state cyber programmes varies. The most advanced nations continue to improve their capabilities at pace, integrating encryption and anonymisation services into their tools in order to remain covert. While they have the technical capability to deploy sophisticated attacks, they can often achieve their aims using basic tools and techniques against vulnerable targets because the defences of their victims are poor.

Only a handful of states have the technical capabilities to pose a serious threat to the UK’s overall security and prosperity. But many other states are developing sophisticated cyber programmes that could pose a threat to UK interests in the near future. Many states seeking to develop cyber espionage capability can purchase computer network exploitation tools ‘off the shelf’ and repurpose these to conduct espionage.

Beyond the espionage threat, a small number of hostile foreign threat actors have developed and deployed offensive cyber capabilities, including destructive ones. These capabilities threaten the security of the UK’s critical national infrastructure and industrial control systems. Some states may use these capabilities in contravention of international law in the belief that they can do so with relative impunity, encouraging others to follow suit. Whilst destructive attacks around the world remain rare, they are rising in number and impact.

**Terrorists**

Terrorist groups continue to aspire to conduct damaging cyber activity against the UK and its interests. The current technical capability of terrorists is judged to be low. Nonetheless the impact of even low-capability activity against the UK to date has been disproportionately high: simple defacements and doxing activity (where hacked personal details are ‘leaked’ online) enable terrorist groups and their supporters to attract media attention and intimidate their victims.

The current assessment is that physical, rather than cyber, terrorist attacks will remain the priority for terrorist groups for the immediate future. As an increasingly computer-literate generation engages in extremism, potentially exchanging enhanced technical skills, we envisage a greater volume of low-sophistication (defacement or DDoS) disruptive activity against the UK. The potential for a number of skilled extremist lone actors to emerge will also increase, as will the risk that a terrorist organisation will seek to enlist an established insider. Terrorists will likely use any cyber capability to achieve the maximum effect possible. Thus, even a moderate increase in terrorist capability may constitute a significant threat to the UK and its interests.

**États ou menaces parrainées par des États**

Nous observons régulièrement des tentatives de pénétration des réseaux britanniques menées par des États et des groupes parrainés par des États en vue d’obtenir un avantage politique, diplomatique, technologique, commercial et stratégique, visant essentiellement les secteurs gouvernementaux, de la défense, des finances, de l’énergie et des télécommunications.

La capacité et l’impact des cyberprogrammes de ces États varient. Les nations les plus avancées continuent de renforcer progressivement leurs capacités, en intégrant des services de chiffrement et d’anonymisation à leurs outils afin de rester dissimulées. Même si elles ont la capacité technique de déployer des attaques sophistiquées, elles peuvent souvent atteindre leurs objectifs à l’aide d’outils et de techniques basiques contre des cibles vulnérables, car les moyens de défense de leurs victimes sont insuffisants.

Seule une poignée d’États ont les capacités techniques de porter sérieusement atteinte à la prospérité et la sécurité globale du Royaume-Uni. Mais bien d’autres États développent des cyberprogrammes sophistiqués susceptibles de menacer les intérêts du Royaume-Uni dans un avenir proche. De nombreux États, cherchant à renforcer leur capacité de cyberespionnage, peuvent acheter des outils d’exploitation de réseaux informatiques dans le commerce et les redéfinir à des fins d’espionnage.

Au-delà de la menace d’espionnage, un petit nombre d’auteurs de menaces étrangères hostiles ont mis au point et déployé des cybercapacités offensives, y compris des capacités destructrices. Ces capacités menacent la sécurité des infrastructures nationales et des systèmes de contrôle industriels stratégiques du Royaume-Uni. Certains États peuvent utiliser ces capacités en violation de la loi internationale et avec la conviction de pouvoir agir en toute impunité, en encourageant les autres à faire de même. Même si les attaques destructrices dans le monde restent rares, leur nombre et leur impact croissent.

**Terroristes**

Les groupes terroristes poursuivent leur objectif de porter atteinte au Royaume-Uni et à ses intérêts à travers leurs cyberactivités. La capacité technique actuelle des terroristes est jugée faible. À ce jour néanmoins, ces actes – même de faible capacité – perpétrés contre le Royaume-Uni ont eu un impact disproportionnellement élevé : de simples dégradations et actes de doxing (diffusion en ligne de données personnelles piratées) permettent aux groupes terroristes et à leurs soutiens d’attirer l’attention des médias et d'intimider leurs victimes.

L’évaluation actuelle révèle que les attaques terroristes physiques, plutôt qu’informatiques, resteront la priorité des groupes terroristes dans le futur immédiat. Face au nombre croissant de terroristes de nouvelle génération bien formés à l'informatique qui s’engagent dans l’extrémisme et échangent potentiellement des compétences techniques, une intensification des perturbations peu sophistiquées (dégradation ou DDOS) ciblant le Royaume-Uni est à prévoir. Il est aussi fort probable de voir émerger de nombreux extrémistes isolés et entraînés, tout comme le risque qu’une organisation terroriste cherche à enrôler une menace interne en place. Les terroristes utiliseront certainement toutes les cybercapacités à leur disposition pour obtenir le maximum d’effets possibles. Ainsi, même une augmentation modérée de la capacité terroriste peut constituer une menace importante pour le Royaume-Uni et ses intérêts.

**Hacktivists**

Hacktivist groups are decentralised and issue-orientated. They form and select their targets in response to perceived grievances, introducing a vigilante quality to many of their acts. While the majority of hacktivist cyber activity is disruptive in nature (website defacement or DDoS), more able hacktivists have been able to in inflict greater and lasting damage on their victims.

**Insiders**

Insider threats remain a cyber risk to organisations in the UK. Malicious insiders, who are trusted employees of an organisation and have access to critical systems and data, pose the greatest threat. They can cause financial and reputational damage through the theft of sensitive data and intellectual property. They can also pose a destructive cyber threat if they use their privileged knowledge, or access, to facilitate, or launch, an attack to disrupt or degrade critical services on the network of their organisations, or wipe data from the network.

Of equal concern are those insiders or employees who accidentally cause cyber harm through inadvertent clicking on a phishing email, plugging an infected USB into a computer, or ignoring security procedures and downloading unsafe content from the Internet. Whilst they have no intention of deliberately harming the organisation, their privileged access to systems and data mean their actions can cause just as much damage as a malicious insider. These individuals are often the victims of social engineering – they can unwittingly provide access to the networks of their organisation or carry out instructions in good faith that benefit the fraudster.

The overall cyber risk to an organisation from insider threats is not just about unauthorised access to information systems and their content. The physical security controls protecting those systems from inappropriate access, or removal of sensitive data or proprietary information on different forms of media, are equally important. Similarly, a robust personnel security culture that is alive to the threat posed by disaffected employees, fraud in the workforce and industrial and other forms of espionage is an important element in a comprehensive approach to security.

**Hacktivistes**

Les groupes d’hacktivistes sont décentralisés et focalisés sur les problèmes. Ils forment et sélectionnent leurs cibles en réponse à des griefs perçus, en introduisant une dimension justicière à bon nombre de leurs actes. Alors que la majorité des cyberactivités menées par les hacktivistes sont de nature à perturber (dégradation de sites Web ou DDOS), des hacktivistes plus compétents sont capables d’infliger des dommages plus importants et durables à leurs victimes.

**MENACES INTERNES**

Les menaces internes demeurent un cyberrisque pour les organisations au Royaume-Uni. Les menaces internes malveillantes, incarnées par des employés de confiance d’une organisation ayant accès à des systèmes et des données stratégiques, représentent le danger le plus sérieux. Elles peuvent causer des dommages financiers et entacher une réputation grâce au vol de données sensibles et de propriété intellectuelle. Elles peuvent aussi constituer une cybermenace destructrice si elles exploitent leurs connaissances privilégiées, ou accès, pour faciliter ou lancer une attaque visant à perturber ou dégrader des services stratégiques sur le réseau de leur organisation, ou effacer des données du réseau.

Autre source de préoccupation similaire : les menaces internes ou employés qui génèrent une cybernuisance à cause d'un clic accidentel sur un courrier d’hameçonnage, insèrent une clé USB infectée dans un ordinateur, ou ignorent les procédures de sécurité et téléchargent du contenu non sécurisé sur Internet. Même si ces employés n’ont pas l’intention de compromettre délibérément l’organisation, leur accès privilégié aux systèmes et données peuvent rendre leurs actions aussi nuisibles qu’une menace interne malveillante. Ces individus sont souvent victimes de l’ingénierie sociale, ils peuvent involontairement fournir un accès aux réseaux de leur organisation ou exécuter des instructions en toute bonne foi au profit du fraudeur.

Le cyberrisque global que représentent les menaces internes pour une organisation ne se limite pas à un accès non autorisé aux systèmes d'information et à leur contenu. Les contrôles de sécurité physique protégeant ces systèmes contre un accès inapproprié ou la suppression de données sensibles ou d’informations propriétaires sur différentes formes de support, sont tout aussi importants. De même, une forte culture de sécurité du personnel érigée contre la menace incarnée par des employés mécontents, la fraude de main-d'œuvre et l’espionnage industriel ou de toute autre nature, est un élément important dans une approche de sécurité globale.

### Case study 1: TalkTalk compromise

On 21 October 2015, UK telecommunications provider TalkTalk reported a successful cyber-attack and a possible breach of customer data. The subsequent investigation determined that a database containing customer details had been accessed via public-facing internet servers, with the records of approximately 157,000 customers at risk, including names, addresses and bank account details. On the same day, several TalkTalk employees received an email with a ransom demand for payment in Bitcoins. The attackers detailed the structure of the database as apparent proof that it had been accessed. TalkTalk’s report of the breach helped the police, supported by specialists at the National Crime Agency, to arrest the main suspects, all based in the UK, in October and November 2015.

The attack demonstrates that, even within large cyber-aware organisations, vulnerabilities can persist. Their exploitation can have a disproportionate effect in terms of reputational damage and operational disruption, and this incident generated substantial media attention. TalkTalk’s rapid reporting of the breach enabled law enforcement to respond in a timely manner, and both the public and government to mitigate the potential loss of sensitive data. The incident cost TalkTalk an estimated £60m and the loss of 95,000 customers, as well as a sharp drop in their share price.

### Étude de cas 1 : compromission de TalkTalk

Le 21 octobre 2015, le fournisseur de télécommunications britannique TalkTalk a signalé une cyberattaque réussie et une possible fuite des données clients. L’enquête qui a suivi a déterminé qu’une base de données contenant les informations des clients avait été consultée depuis des serveurs Internet publics. Cette base contenait les dossiers d’environ 157 000 clients ainsi exposés au risque, y compris les noms, adresses et coordonnées bancaires. Le même jour, plusieurs employés de TalkTalk ont reçu un courriel avec une demande de rançon pour un paiement en bitcoins. Les assaillants ont décrit en détail la structure de la base de données comme preuve concrète de leur intrusion. Le rapport de TalkTalk sur la fuite de données a aidé la police, assistée de spécialistes de l’Agence nationale contre le crime, à arrêter les principaux suspects, tous résidant au Royaume-Uni, en octobre et novembre 2015.

L’attaque démontre que, même au sein des grandes organisations sensibilisées aux questions informatiques, des vulnérabilités peuvent subsister. Leur exploitation peut avoir un impact disproportionné en termes d’atteinte à la réputation et de perturbation opérationnelle. Cet incident a fortement attiré l’attention des médias. Le signalement rapide de la fuite par TalkTalk a permis aux forces de l’ordre de réagir rapidement et au public et au gouvernement de limiter la perte potentielle de données sensibles. L’incident a coûté environ 60 millions de livres sterling à TalkTalk et causé la perte de 95 000 clients, ainsi que la chute vertigineuse du prix de ses actions.

### Case study 2: attack on Bangladesh Bank’s swift system

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure way. As SWIFT sends payment orders which must be settled by correspondent accounts that the institutions have with each other, there has long been concern over any potential for this process to be compromised by cyber criminals or other malicious actors, seeking to inject illegitimate payment orders into the system or, in a worst case scenario, seeking to disable or disrupt the functionality of the SWIFT network itself.

In early February 2016, an attacker accessed the SWIFT payment system of the Bangladesh Bank and instructed the New York Federal Reserve bank to transfer money from Bangladesh Bank’s account to accounts in the Philippines. The attempted fraud was US$951 million. 30 transactions, worth US$850 million, were prevented by the banking system; however, five transactions worth US$101 million went through. US$20 million, traced to Sri Lanka, has since been recovered. The remaining US$81 million transferred to the Philippines was laundered through casinos and some of the funds were then forwarded to Hong Kong.

The forensic investigation launched by Bangladesh Bank discovered that malware had been installed on the bank’s systems and had been used to gather intelligence on the procedures used by the bank for international payments and fund transfers. Further analysis by BAE Systems of the malware linked to the attack uncovered sophisticated functionality for interacting with the local SWIFT Alliance Access software running in the Bangladesh Bank infrastructure. BAE concluded ‘that criminals are conducting more and more sophisticated attacks against victim organisations, particularly in the area of network intrusions’.

### Étude de cas 2 : attaque du système swift de la Banque du Bangladesh

Le système SWIFT (Society for Worldwide Interbank Financial Telecommunication) fournit un réseau qui permet aux institutions financières internationales d’envoyer et de recevoir des informations sur les transactions financières en toute sécurité. Alors que le SWIFT envoie des ordres de paiement qui doivent être réglés par les comptes correspondants que les institutions se partagent, il existe depuis longtemps une préoccupation sur le potentiel de compromission de ce processus par des cybercriminels ou d’autres acteurs malveillants cherchant à injecter des ordres de paiement illégaux dans le système ou, dans un scénario catastrophe, à désactiver ou perturber les fonctionnalités du réseau du système SWIFT lui-même.

Début février 2016, un assaillant a accédé au système de paiement SWIFT de la Banque du Bangladesh et a donné l’ordre à la banque de la Réserve fédérale de New York d’effectuer un transfert d’argent du compte de la Banque du Bangladesh vers des comptes basés aux Philippines. La tentative de fraude s’est élevée à 951 millions de dollars américains. Le système bancaire a empêché 30 transactions d’une valeur de 850 millions de dollars américains. Cependant, cinq transactions d’une valeur de 101 millions de dollars américains ont réussi. 20 millions de dollars américains, localisés au Sri Lanka, ont depuis été récupérés. Les 81 millions de dollars américains restants transférés aux Philippines ont été blanchis dans les casinos et certains de ces fonds ont ensuite été transférés à Hong-kong.

L’enquête judiciaire initiée par la Banque du Bangladesh a révélé qu’un logiciel malveillant avait été installé sur les systèmes de la banque et avait servi à collecter des renseignements sur les procédures utilisées par la banque pour les paiements internationaux et les transferts de fonds. BAE Systems a mené une analyse approfondie du logiciel malveillant impliqué dans l’attaque et dévoilé une fonctionnalité sophistiquée qui permettait d’interagir avec le logiciel local SWIFT Alliance Access exécuté dans l’infrastructure de la Banque du Bangladesh. BAE a conclu que « ces criminels mènent des attaques de plus en plus sophistiquées contre des organisations victimes, particulièrement dans le domaine des intrusions de réseaux ».

### Case study 3: Ukraine power grid attack

A cyber-attack on western Ukrainian electricity distribution companies Prykarpattya Oblenergo and Kyiv Oblenergo on 23 December 2015 caused a major power outage, with disruption to over 50 substations on the distribution networks. The region reportedly experienced a blackout for several hours and many other customers and areas sustained lesser disruptions to their power supplies, affecting more than 220,000 consumers. Use of the BlackEnergy3 malware has been blamed by some for the attack, after samples were identified on the network.

At least six months before the attack, attackers had sent phishing emails to the offices of power utility companies in the Ukraine containing malicious Microsoft Office documents. However, the malware was not likely to have been responsible for opening the circuit breakers which resulted in the outage. It is probable that the malware enabled the attackers to gather credentials that allowed them to gain direct remote control of aspects of the network, which would subsequently enable them to trigger the outage. This Ukraine incident is the first confirmed instance of a disruptive cyber-attack on an electricity network. Instances such as this further demonstrate the need for good cyber security practices across all of Critical National Infrastructure (CNI).

### Étude de cas 3 : attaque du réseau électrique ukrainien

Une cyberattaque perpétrée contre les entreprises de distribution électrique ukrainiennes Prykarpattya Oblenergo et Kyiv Oblenergo le 23 décembre 2015 a causé une importante panne électrique et perturbé plus de 50 sous-stations sur les réseaux de distribution. La région a signalé une panne de courant de plusieurs heures et un grand nombre d’autres clients et zones ont relevé des perturbations moindres sur leurs réseaux électriques, affectant plus de 220 000 clients. L’utilisation du logiciel malveillant BlackEnergy3 a été mise en cause par certains dans l’attaque, après que des échantillons ont été identifiés sur le réseau.

Au moins six mois avant l’attaque, les assaillants avaient envoyé des courriers d’hameçonnage aux bureaux des compagnies d’électricité en Ukraine contenant des documents Microsoft Office malveillants. Cependant, le logiciel malveillant n’est probablement pas à l’origine de l’ouverture des disjoncteurs qui a entraîné la panne. Il est probable que le logiciel malveillant ait permis aux assaillants de récupérer les identifiants de connexion et de prendre directement le contrôle à distance des éléments du réseau, ce qui les aurait aidés par la suite à déclencher la panne. Cet incident en Ukraine est le premier exemple avéré de cyberattaque causant des perturbations sur un réseau électrique. Ce genre d’exemple confirme le besoin d’instaurer de bonnes pratiques de cybersécurité dans toutes les infrastructures nationales critiques (CNI).

Version/Date