

CYBER CRISIS MANAGEMENT
COLLECTION

ANTICIPATING AND MANAGING CYBER CRISIS COMMUNICATION



CYBER CRISIS MANAGEMENT
SERIES

A GUIDE

ANTICIPATING AND MANAGING CYBER CRISIS COMMUNICATION

Founded in 2009 as a Prime Minister's office placed under the authority of the Secretary-General of Defence and National Security, the French Cybersecurity Agency (ANSSI) is the national authority in matters of cybersecurity and cyber-defence. The French cybersecurity model establishes a clear distinction between defensive and offensive missions and, within this framework, ANSSI is responsible for coordinating the defence and protection of information systems.

ANSSI's primary purpose is to design and organise the state's protection against cyberattacks, at the interministerial level, and to contribute to the stability of cyberspace. It acts in line with the state's core functions, working towards the general goal of a public policy for the security and resilience of administrations, the economy, and society as a whole.

ANSSI'S ACTIVITIES MAY BE BROKEN DOWN INTO THREE OVERARCHING MISSIONS

Defending

critical information systems and victims
of large-scale cyberattacks

Keeping informed

of the state of the art in matters of cybersecurity
and of the threats looming over cyberspace

Sharing

knowledge, recommendations,
and expertise in digital security

Supporting

the national and
international ecosystem

Regulating

cybersecurity organisations,
products, and services

TABLE OF CONTENTS

INTRODUCTION	8
BEFORE A CYBER CRISIS	10
Section 1: Initiating internal dialogue and anticipating scenarios.....	11
Section 2: Assembling a dedicated toolbox.....	14
Section 3: Training teams	17
DURING A CYBER CRISIS	20
Section 4: Organising cyber crisis communication.....	21
Section 5: Defining a cyber crisis communication strategy.....	26
Section 6: Formulating keys messages.....	41
Section 7: Managing internal crisis communication	52
Section 8: Managing external crisis communication.....	56
AFTER A CYBER CRISIS	70
Section 9: Thanking associates and reviewing experience feedback.....	71
Section 10: Sharing experience feedback and raising awareness amongst associates.....	73
CHECKLIST	76
RESOURCES	78

INTRODUCTION

In the event of an attack, the technicality of a cyber crisis may destabilise even the most seasoned of communicators, faced with an ecosystem, codes, and stakes which can sometimes differ significantly from what they are typically used to.

While it focuses on the specificities of the cyber field, the present guide endeavours to demonstrate that proper cyber crisis communication primarily hinges on the common reflexes and tools inherent to every crisis communication strategy.

→ WHAT IS THE PURPOSE OF THIS GUIDE?

Drawing on the different cases encountered by ANSSI while assisting victims, this guide is intended to provide operational recommendations which might be used to anticipate and implement crisis communication strategies during cyberattacks. While there is no magic formula for crisis communication, there are essential notions and reflexes which can already be integrated by your entity to prepare to face potential cyber crises. This guide comprises practical guidelines broken down into ten distinct sections, as well as a checklist of best practices and of pitfalls to avoid. It also presents the testimonies of communicators from several different public and private entities.

→ WHO IS IT INTENDED FOR?

This guide is intended for any individual involved in communication efforts during the management of a cyber crisis impacting a public administration, private enterprise, or association (referred to as an “entity” henceforth). This individual may be a communications professional (communications director, communications officer, or communications agency) or, wherever there exists no designated communicator, they may also have a different background (director/chief of staff, secretary-general, legal expert, etc.).

AND WHAT IS A CYBER CRISIS?

A “cyber crisis” is characterised by the immediate and significant destabilisation of an entity’s usual operations (shutdown, inability to provide services, heavy financial losses, major loss of integrity, etc.), caused by one or several malicious actions against its digital services and tools (ransomware attacks, denials of service, etc.). It is a high-impact event which cannot be handled through the usual processes or within the framework of the entity’s standard operations. From here on out, these events will be referred to as “cyber crises”.

BEFORE A CYBER CRISIS

The effective management of crisis communication primarily hinges on anticipation. Before a crisis strikes, when conditions are stable and conducive to reflection and change, the best practices presented in the sections below may be adopted at each entity's own pace.

Section 1: Initiating internal dialogue and anticipating scenarios	11
Section 2: Assembling a dedicated toolbox	14
Section 3: Training teams	17

SECTION 1 BEFORE A CYBER CRISIS



INITIATING INTERNAL DIALOGUE AND ANTICIPATING SCENARIOS

When a cyber crisis strikes, the cyber/IT team – including the Chief Information Security Officer (CISO) and the Data Protection Officer (DPO) – and the communications team are both heavily mobilised. These can be difficult conditions for the two to get acquainted in.

To ensure relevant cyber crisis communication, it is therefore crucial to proactively initiate dialogue between cyber/IT and communications teams. The goal is for the two teams to get to know each other and to develop a better understanding of their respective priorities, challenges, and vocabulary. The head of IT is able to provide real-time reports of the technical situation and its potential developments, while the communicator possesses extensive knowledge of the entity's (internal and external) target audiences and means of communications. This process of mutual acculturation may take various forms:

- **Dedicated workshops.**
- **Internal awareness-raising campaigns**, during “Cybermonth”, for example, which takes place in October of each year to raise public awareness of cybersecurity and promote best practices.
- **Cyber crisis management exercises¹.**

¹ For more information, see ANSSI's guide [Organising a cyber crises management exercise](#).

Each entity must also conduct an analysis of the risks threatening to destabilise their operations². Actors involved in crisis management and cyber/IT teams must anticipate several realistic crisis scenarios (DDoS, ransomware, defacement, etc.). It is then recommended to prepare crisis communication strategies (**see Section 5**) for each of the identified scenarios, to be put to the test during a crisis management exercise. Even without seeking to be exhaustive, anticipating these communication strategies will set the groundwork for the swift and effective implementation of measures when crisis does strike.



If an entity does not possess its own cyber/IT team, external service providers and resources such as [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)³ can provide the means to better understand cybersecurity.

² For more informations, *EBIOS Risk Manager-The method*.

³ Launched in 2017, the [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr), platform is a national tool for awareness-raising, prevention, and the assistance of cyber-maliciousness victims. It is intended for individuals, companies, and local governments.

“The regular acculturation of communications teams to the various existing forms of cyberthreat significantly facilitates coordination in the event of a crisis.”

Laurent Baude
Head of Sensitive and Crisis Communications,
RATP Group



REMEMBER It is crucial for communications and cyber/IT teams to meet prior to the occurrence of cyber crisis, so that they may develop a better understanding of their respective priorities, challenges, and vocabulary. On the basis of the different plausible cyber crisis scenarios identified (DDoS, ransomware, defacement, etc.), it is recommended to prepare different communication strategies.

SECTION 2 BEFORE A CYBER CRISIS



ASSEMBLING A DEDICATED TOOLBOX

To prepare for a cyber crisis, it is recommended to gather useful resources in a dedicated toolbox. This toolbox should allow the swift implementation of effective cyber crisis communication measures when a crisis does occur. It may contain the following components:

- **Pre-identified crisis communication strategies, along with the associated language elements (see Sections 5 and 6)** formulated on the basis of different plausible cyber scenarios (see Section 1). ANSSI's *CyberDico* can be a useful resource in the conception of this document. It can be freely accessed through ANSSI's website and lists, in alphabetical order, the various terms, phrases, and acronyms used in cybersecurity. It is regularly updated and contains both French and English definitions.
- **A computer that is either completely blank or disconnected from the network** (to use DTP tools or social network accounts, send internal communications, etc.).
- **Your entity's crisis management framework and the directories of crisis management team members.**
- **A listing of degraded modes of communication.**
A listing of degraded modes of communication. Before a cyber crisis occurs, it is crucial to anticipate degraded modes of internal and external communication; in the event of a cyberattack, the entity's usual communication tools may be impacted and rendered unusable. To achieve this, an extreme situation must be conceived: how to communicate without Internet and/or without access to emails and/or without phones and/or without

being able to access servers? **Section 8** provides some tips for the development of degraded modes of communication.

→ **Codes and tools to manage communication:**

- ▶ account login codes (social media accounts, mobile applications, website, intranet, etc.)
- ▶ communications templates (press releases, social media publications, etc.)
- ▶ a directory of the entity's spokespersons
- ▶ a file containing the contact information of journalists and influencers

To prepare this toolbox, the entity's disaster recovery plan (DRP) or business continuity plan (BCP) may also be used. Established as means to deal with identified risks, these plans hinge on specific resources and procedures identified prior to the situations encountered.

The toolbox must be regularly updated to take into account real or fictitious feedback drawn, for instance, from a cyber crisis exercise. It should be available on one of the entity's computer servers (in case these remain accessible during a crisis), a USB stick, a digital vault, and in a print form in case digital versions are rendered inaccessible, due to a cyberattack for example.

“The anticipation and management of a crisis hinges on the thorough preparation and organisation of teams, as well as on processes defined and established ahead of time.”

Caroline de Lastic
Head of Strategic Coordination and Corporate Communication,
Naval Group



FOCUS **THE SECURITY OF SOCIAL** **MEDIA ACCOUNTS IS PARAMOUNT**

- Choose a unique, robust password for each social media platform (at least 12 characters, including uppercase and lowercase letters, numbers, and special characters), and use a password manager.
- Avoid logging into social media accounts using free Wi-Fi networks.
- Separate uses and do not connect the entity's social media accounts to personal accounts.
- Systematically enable the double authentication feature provided by social media platforms, which requires a second authentication factor (by SMS, email, or, ideally, via a dedicated application) whenever a new device is used.
- Regularly renew passwords.
- Avoid leaving unprotected written records of passwords when these must be shared between associates.



REMEMBER

A dedicated cyber crisis communication toolbox must be assembled before a crisis strikes, comprising pre-identified cyber crisis communication strategies and the associated language elements, the crisis management framework, a listing of degraded internal and external modes of communication, and codes and tools to manage communication.

SECTION 3 BEFORE A CYBER CRISIS



TRAINING TEAMS

Cyber crisis management exercises provide an opportunity for entities to test, in the context of a large-scale attack paralysing their information systems, the maturity and resilience of their communications team, as well as their cyber crisis communication framework. These exercises make it possible to automate actions and ultimately save time in the event of a real incident – particularly with regard to communication.

Based on the scenarios formulated with the cyber/IT and crisis management teams, different types of exercises may be organised:

- **A global, entity-wide exercise:** this type of exercise allows entities to test their communications teams' ability to work with their crisis management framework in the event of a cyber crisis. It is also an opportunity to test the preparedness of their communications teams when faced with the different scenarios conceived.
- **An exercise specifically dedicated to communication:** this type of exercise allows communications teams to familiarise themselves with the realm of cybersecurity and to test out their modes of action.

Such exercises should be performed on a regular basis to ensure the proper training of associates (particularly following renewals) and to test out new tools and procedures. These new tools and procedures can be effective when preparations are made beforehand (*see Sections 1 and 2*) and feedback is reviewed to allow teams to progress⁴ (*see Section 9*).

⁴ For more information, see ANSSI's guide on *Organising a cyber crisis management exercise*.

A cyber crisis management exercise may be arranged internally by the entity, or by a service provider specialised in crisis management⁵. To ensure the success of an exercise, it may be useful to include simulated media pressure: simulated media calls, fake press reports, or even fake posts on fake social media platforms.



Proactive media training is one of the keys to successful cyber crisis communication. Filmed simulated interviews and Q&A sessions allow spokespersons to better grasp the media's expectations in the event of a cyberattack, and to fine-tune their messages. Media training therefore allows communicators to develop reflexes which will prove invaluable when a media crisis occurs, as the time required to prepare an interview will likely be reduced.

⁵ For more information, see the PACS (Cybersecurity support and consulting service provider) requirements framework.

“Training for cyber crises does not signify a fear of the unforeseen; it is simply a decision to not endure them. Ultra-realistic scenarios, committed teams, honed reflexes... When crisis strikes, we act collectively – and this makes all the difference!”

Armelle Calippe

Head of Communications, Press and Institutional Relations,
France Titres – Agence nationale des titres sécurisés



REMEMBER

It is highly recommended to take part in a cyber crisis exercise in order to test the resilience of the communications team and its tools when confronted with a cyberattack. Media training allows spokespersons to develop reflexes which will prove invaluable when a media crisis occurs.

DURING A CYBER CRISIS

Crisis has struck. The (operational and strategic) crisis management units have been activated. The communications team is called upon to contribute its expertise to the management of the crisis. The following sections present the best practices to implement at this stage.

Section 4: Organising cyber crisis communication 21

Section 5: Defining a cyber crisis communication strategy 26

Section 6: Formulating key messages 41

Section 7: Managing internal crisis communication 52

Section 8: Managing external crisis communication 56

SECTION 4 DURING A CYBER CRISIS



ORGANISING CYBER CRISIS COMMUNICATION

Whether the crisis be of cyber origin or not, crisis communication should be integrated into the entity's crisis management framework within the first few hours. Communicators have several roles to play and missions to fulfil.

If the entity possesses an internal communications team, a crisis-specific organisational framework should be quickly established from the offset of the cyber crisis, with the distribution of the following roles and missions.

COORDINATION

The communicator must be fully integrated into the crisis unit(s) to assist entity heads in the choice of a communication stance. They should also ensure that outbound communications meet the objectives laid out by the entity and match the timings of the different actors involved.

The integration of communicators in the different crisis units will make it possible, at the outset and during the cyber crisis, to:

- **Understand** the observations made, the context of the cyber crisis, and the situation in which the entity finds itself with regard to communication (**see Section 5**).
- **Share** their perception of the situation (media and internal monitoring) to fuel the entity's global risk analysis.
- **Define** a communication stance.
- **Centralise** in-house and external productions and obtain their validation.
- **Connect** with external stakeholders.

PERCEPTION

The communicator must then be attentive to media and social media reactions to matters linked to the entity (see Section 8).

- **In the run-up to the cyber crisis**, monitoring can allow the detection, particularly on social media, of faint signals alerting to a technical incident (post by an influencer, claiming of an attack, etc.). In this case, the communicator should notify the implicated stakeholders (entity heads, the cyber/IT team, etc.).
- **At the outset and during the cyber crisis**, a media and social media monitoring system should be established and ideally maintained by a dedicated person. It is also beneficial to monitor any political speeches and the reactions of in-house staff (alongside the in-house communications officer). This media monitoring will lay the groundwork to develop and adapt the entity's communication stance.

REACTION

The communicator must control the diversity of the entity's audiences, whether they be internal or external, as well as the tools available to it. This expertise is invaluable to enhance the entity's responsiveness.

- **At the outset of the cyber crisis**, messages specifically tailored to the different targeted audiences, whether internal or external, must be swiftly formulated, with the support of the implicated business teams. The communicators in charge of media relations, of social media, of the entity's website, and of internal communications adapt and relay these messages to their respective audiences (see Sections 7 and 8).
- **During the cyber crisis**, communication should be dynamic and tailored to the specific reactions of target audiences (see "Perception").

These roles may be compiled in a single crisis communications unit. It is important to anticipate this cyber crisis mode of organisation to prepare for a potential incident.

If the communications team is understaffed, some of its officers will be required to shoulder several roles at once. If that is not enough, it may be necessary to call for in-house or external reinforcements. If an entity does not possess a communications team and/or if its communication is outsourced (handled by a service provider), it will require assistance to fulfil the aforementioned missions. Various different actors offer cyber crisis communication support: security incident response service providers (PRIS) qualified by ANSSI, and consulting agencies or firms specialised in crisis communication. In cases of incidents monitored by the CERT-FR, cyber crisis communication support may also be offered by ANSSI.

During the cyber crisis, it is recommended to establish a swift hierarchical validation chain (who is responsible for alerting who, who makes the decisions, etc.), a rotation system for the communications team's key positions, and even to identify staff members from other teams capable of serving as reinforcements.

Note: when a cyber crisis first strikes, it is a good idea to start a log of all events linked to the incident and of the communication measures implemented. Each log entry should at least include:

- **The time and date of the event or of the measure's implementation**
- **The name of the person who is responsible for the measure or who reported the event**
- **A description of the measure or event**



FOCUS

3 USEFUL SOFT SKILLS FOR THE MANAGEMENT OF CRISIS COMMUNICATION

1

PRIORITISING CALMNESS

Adopting a positive and calm attitude greatly simplifies the resolution of a crisis. It is also important to protect the cyber/IT team from media inquiries so that it may work in peace.

2

BEING FLEXIBLE

In unprecedented situations, the BCP may not suffice on its own. The communicator must therefore be flexible and think “out of the box” to develop new means of communication.

3

TAKING CARE OF ONESELF

A cyber crisis often gives rise to internal tensions and communicators can, at times, be put under a lot of pressure. It is therefore important to take a step back from the situation in order to better face it. For the sake of your health, allow yourself moments of relaxation.

“The establishment of a crisis unit – and more particularly of a dedicated communications unit – is a major asset. It is the key to ensuring coherent, controlled communication at the appropriate level, developed alongside experts as our cyber teams remain focused on the analysis and operational management of the incident.”

Bertrand Le Piolot
Group Cybersecurity Director,
FDJ UNITED



REMEMBER

A specific organisational framework may be established at the beginning of the cyber crisis, with the distribution of roles (coordination, perception, and reaction) and missions. In cases where resources are insufficient or lacking entirely, support may be obtained from security incident response service providers (PRIS), consulting agencies or firms specialised in crisis communication, or, in some cases, ANSSI.

SECTION 5 DURING A CYBER CRISIS



DEFINING A CYBER CRISIS COMMUNICATION STRATEGY

1 TAKING STOCK OF THE SITUATION

There is no one-size-fits-all approach to cyber crisis communication. The most suitable strategy will be determined by the facts, the situation in terms of communication, and the context in which the cyber crisis has occurred. At the start of a cyber crisis, the communicator must take stock of the situation and gather the essential information listed below.

FACTS ESTABLISHED

- **Request a report of the situation to better understand the incident, as there exist different types of cyberattacks.** Try to learn more about the incident's business impact, as well as its impact on services/tools. The goal is to figure out if the attack itself is visible to the entity's internal and external audiences (for example: ransomware and denial of service attacks are highly visible, while espionage operations are not), or if its impacts are visible (for example: the entity is unable to pay its staff or to maintain its usual services).
- **Summarise the first measures taken by the entity regarding the different aspects of its operations:** technical, legal, communication, and even organisational.

THE SITUATION IN TERMS OF COMMUNICATION

- **Review the entity's global communication strategy** to formulate a crisis communication strategy which remains consistent with the entity's identity, objectives, and priority targets.
- **Take stock of the communication channels which remain available in spite of the cyberattack** (social media, website, internal messaging system, etc.) or with significant constraints (for example: channels only accessible via offline workstations).
- **Request a situation report on the subject's perception internally, in the media and on social media**, including the initial reactions of staff members, clients, users, and suppliers. A cyberattack can become highly viral, and many social media "experts" or specialised journalists may quickly and publicly react to the situation.
- **Take into consideration the number of media inquiries received** by the entity's press office, along with the issues addressed.
- **Ask the Data Protection Officer (DPO) or the legal department if any legal obligations might require the entity to inform stakeholders** (for example, under the General Data Protection Regulation (GDPR) in cases of data theft). Provided for in a statutory provision, this information should be enforced in addition to public crisis communication and may impact the timing of communications.
- **Find out if stakeholders have already communicated on the incident.** This may include the National Commission for Informatics and Liberties (CNIL), the J3 Cybercrime section of the Paris Prosecutor's Office, regulation or sectoral authorities, clients, users, partners, service providers or, in rare cases, ANSSI. Political figures may also communicate on cyber crises, and will sometimes visit the victims.

- **Assess the visibility of attackers.** Certain groups of attackers stand out with specific communication strategies, such as the automatic claiming of attacks or the threatened publication of exfiltrated data. These initiatives can be more or less visible depending on the communication channel used by the attacker. The attacker may communicate via a showcase website on the dark web, encrypted messaging, and even press releases or social media. Note that attackers may also directly contact journalists or the entity's staff members and various departments, including its press department (in-house or outsourced), by email or by phone, to exert further pressure on the victim and to encourage a hasty reaction.

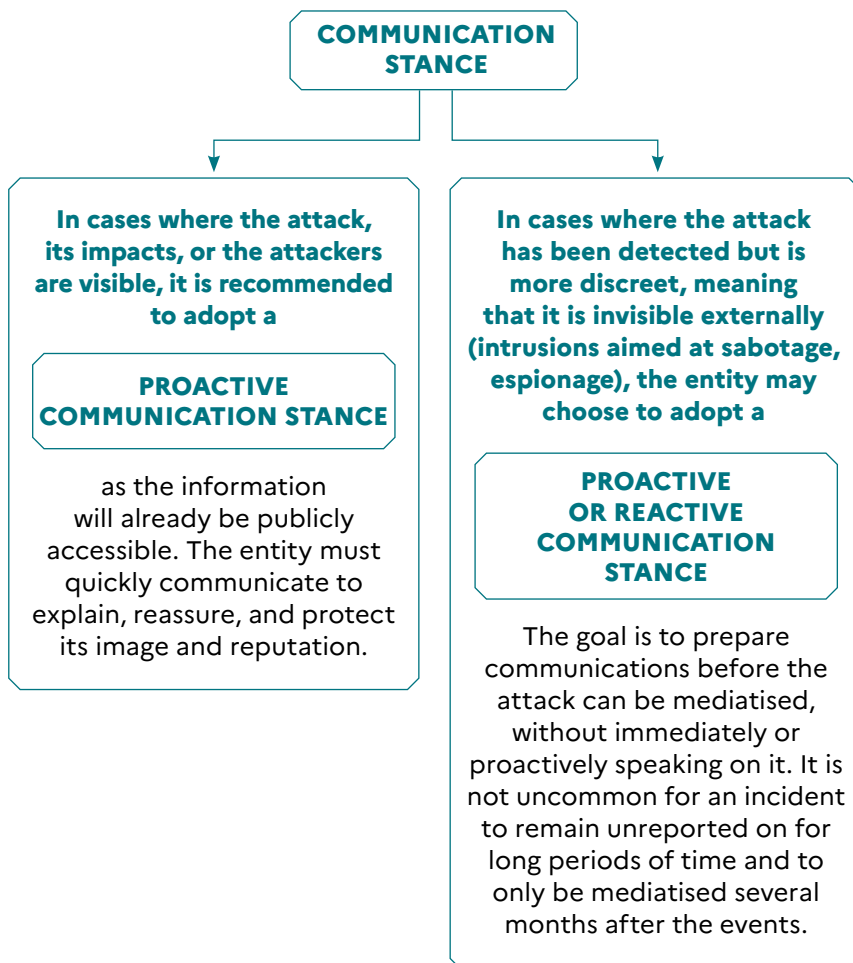
CONTEXT

Identify any matters of concern, in view of the context in which the entity operates:

- **The entity's current events.** For example: a significant upcoming communication campaign, the forthcoming publication of financial results, ongoing wage negotiations, the upcoming launch of a product, and even the acquisition of the entity.
- **The socio-economic and political context in which the entity operates,** with a major sector-specific event in preparation or an ongoing or upcoming election period.

2 COMMUNICATION STANCE

Once the situation has been taken stock of, the entity must define and present a communication stance (proactive or reactive) to its executives.



It is important to keep in mind that the communicator only presents a communication stance to include in the general (human, financial, legal, reputational, etc.) cost/benefits analysis conducted by the entity's stakeholders. The responsibility of deciding on a stance befalls the entity's executives, who must accept short and medium-term risks.

This communication stance should be reassessed over the course of the cyber crisis management process, in view of the incident's evolving context, to reorient communication measures accordingly.

“By virtue of their interdependence and immediacy, cyber crises require an approach to communication which is based on objectivity and pedagogy, structured around a multidimensional strategy involving every one of the company's stakeholders.”

Marie-Laure Fraux
Communications Advisor,
Banque de France



FOCUS COMMUNICATING ON PROFIT-MOTIVATED CYBERATTACKS

Ransomware is a type of malware used to pressure the victim into paying a ransom. It is one of the tools used by cybercriminals motivated by monetary gain. In cases of ransomware attacks, attackers will put the victim's computer or information system out of service – reversibly or irreversibly. In practice, most ransomware uses cryptographic mechanisms to encrypt the computer or system's data, making it impossible for it to be viewed or used. Once the data has been encrypted, the attacker sends an unencrypted message to the victim offering to provide the means to decrypt the data in exchange for the payment of a ransom.

This type of attack has two main characteristics which set it apart from more discreet attacks:



THE PACE

an almost immediately and systematically visible attack

A ransomware attack is likely to be immediately made public due to the impact it can have (example: impossibility of providing a service to clients or users), because of an information leak occurring after the sharing of screen grabs from the entity with the public or with cybercriminal groups developing an attack-based approach to public communication to exert pressure on their victim (blackmail for decryption, the publication of a sample, or the reselling of data).



THE TOOLS

possible paralysis of traditional communication tools

Depending on the extent of the incident's propagation, the entity's IT tools may become partially or completely unavailable – making it impossible to access the communicator's usual tools (press files, social media accounts, website, emails, etc.) and impeding the implementation of quick communication measures (internal email or message, emails to clients/users, etc.).

These characteristics often make it necessary for the communicator to opt for a proactive communication stance, from the offset of the incident, to limit the impact of the cyber crisis on the entity's image and reputation, both in-house and externally.



FOCUS COMMUNICATING ON AN ATTACK AIMED AT ESPIONAGE

Cyberattacks are not always visible. Particularly discreet and sophisticated, attacks aimed at espionage can have disastrous consequences. Attackers may penetrate information systems, sometimes for several years, to steal strategic data.

This type of attack is sometimes detected by chance, sometimes belatedly, and remediation is often a long process as attackers sometimes obtain elevated rights on the information system. In such cases, in-depth technical measures have to be implemented to eject the attacker and improve the information system's security. Reacting to this type of cyberattack also entails interacting with an adversary: the entity's actions and their effects may be observed and interpreted by the attacker. The attacker's reaction can vary depending on their skill, persistence, and aggressiveness levels.

The entity's approach to communication should therefore differ depending on the type of attack, as both in-house and external interactions (between crisis managers, with the entity's teams, or with partners, clients/users, or providers) are potential sources for information for the attacker. Accordingly, it is important for the entity not to "show its cards" and to control the information which might reach the attacker, to hinder their ability to adapt or react.

Generally reactive, an entity's communication stance is determined by the degree of caution to be exercised when implementing remediation measures in order to keep them out of the attacker's line of sight. In-house communication, on the one hand, must be measured to avoid compromising ongoing remediation activities. For external communication, on the other hand, it is recommended not to communicate before the attacker has been ejected from the information system. However, certain key messages must nonetheless be drafted (though they should not be hosted on the information system) and ready to broadcast.

It is recommended to refer to ANSSI's guide "Cyberattacks and Remediation: Preparing for Remediation"⁶ for more information on this topic.

⁶ "Guide only available in French".



FOCUS COMMUNICATING ON AN ATTACK AIMED AT DESTABILISATION

Some cyberattacks, such as distributed denial of service attacks (DDoS) or website defacements, are primarily intended to destabilise the targeted entity. Distributed denials of service prevent or significantly undermine a system's ability to provide an expected service. This action may be malicious, or it may be the result of the service's improper scaling. A distributed denial of service refers to an attack during which a network of (often compromised) devices is used to disrupt one or several targeted services. A defacement results from malicious activity which involves the modification of an Internet server's appearance or content and which undermines the integrity of the webpages by altering them.

These attacks have real business impacts, leading to the malfunction of the services offered, with financial costs which can prove to be significant. Given that they are relatively unsophisticated, however, they can be quickly detected and generally do not have any long-term repercussions (such as data loss or the destruction of the information system). They do however have a significant symbolic and emotional impact: they bring to light a service's vulnerabilities and can even provide a platform for attackers to convey alarming messages. When this type of unsophisticated attack occurs, or in the event of a "false incident", a more significant media crisis may arise and prove more difficult to manage than the technical incident itself. A proactive approach to communication is therefore essential: it is intended to pedagogically explain the – generally moderate – impact of the attack, to quickly reassure the concerned public. Without measured and tailored communication, these attacks may successfully destabilise the entity by provoking a media frenzy.

3 COMMUNICATION OBJECTIVES

Once the situation has been taken stock of and a communication stance has been settled on, the entity may define its communication objectives. The primary objectives to meet during a cyber crisis are as follows:

EXPLAINING AND INFORMING

Educate audiences on the type of attack faced by the entity and on the remediation measures to be implemented in response, promoting a better understanding of events and the sharing of knowledge.

REASSURING

Demonstrate that the entity is doing what needs to be done in order to quickly resolve the cyber crisis, thereby maintaining the trust of clients, users, and in-house associates.

PRESERVING THE ENTITY'S IMAGE AND REPUTATION

Limit the impact of the incident on the entity's reputation through transparent communication
(see Section 9).

It is also necessary to prevent rumours or false information from spreading
(see Section 8).

PROMOTING A CHANGE IN HABITS

Encourage associates to implement security best practices in future uses.

4 TARGET AUDIENCES

During a cyber crisis, the usual targets of communications are:

IN-HOUSE

- **Employees** (or only those whose data has been exfiltrated or even published in the event of data theft)
- **Managers, executive/management committees, directors**
- **Service providers working internally**
- **Subsidiaries or parent entities**
- **Employee representative bodies** (social and economic committee, syndicates, employee representatives, etc.)
- **Spokespersons**

EXTERNAL

- **Journalists** (national and regional journalists, general or specialised in cybersecurity/tech or in the impacted sector)
- **Influencers of the cyber field or of the impacted sector**
- **Prospects**
- **Clients** (can be split up into two categories:
VIP clients and other clients)
- **Users**
- **Service providers**
- **Suppliers**
- **Shareholders and members of the board of directors**
- **Partners** (French, European, international)
- **General public**
- **Individuals whose data has been exfiltrated or published**
(in the case of data theft)
- **ANSSI and the CERT-FR**, particularly if the entity is subjected to regulatory requirement
- **Sector-specific authorities**

- **Political and supervisory authorities, ministerial offices**
- **Technical counterparts** (Sectoral, ministerial, or territorial CSIRTs, InterCERT France, CERT-EU)
- **CNIL**
- **J3 Cybercrime Section of the Paris Prosecutor's Office**

If some of the entity's stakeholders (associates, clients, users, etc.) are based abroad, it is crucial to remember the importance of quickly translating content (at the very least in English).

Note that the communicator is not meant to centralise the drafting and dissemination of communications to the entity's various target audiences. The role of the communicator is to coordinate statements to ensure the cohesiveness, clarity, and command of the entity's overall communication. Every actor plays their own role in the context of these attributions, but nonetheless follows a single collective vision, validated and shared across the entity.

5 PACE OF COMMUNICATION

The pace of a cyber crisis can be difficult to explain: while the attack or its impact can sometimes be immediately visible, analysis methods take time – as does the implementation of remediation measures. Though this argument can be frustrating to hear, it is generally understood by media outlets specialised in cybersecurity. It is, however, less understood by other target audiences. As such, it is important to keep a few tips in mind regarding the pace of communication.

IN THE CASE OF A REACTIVE APPROACH TO COMMUNICATION

- Question the moment and relevance of the entity's first (internal or external) communication after taking stock of the situation (the facts, the situation in terms of communication, and the context in which the cyber crisis occurs).

IN THE CASE OF A PROACTIVE APPROACH TO COMMUNICATION

- **Communicate quickly** as, in our modern society, social media and round-the-clock news channels have made instantaneous information distribution a central characteristic of crisis communication. At the start of a cyber crisis, little verified information is generally available. As such, the entity's first communication can remain short and simply convey that its teams are aware of the incident and actively working towards its resolution. Whatever the case may be, unverified information should never be communicated as it may end up working against the entity's best interest and create bad buzz.
- **At the beginning of the incident, avoid providing a specific recovery date** as unexpected developments may arise (for example: the attacker strikes again and initiates a re-encryption, the cyber/IT teams face technical difficulties during remediation, etc.). **Stakeholders may be kept regularly informed** as the cyber crisis progresses, providing visibility with regard to the different stages of investigation and remediation (as soon as remediation is under control).

- **Prioritise communications depending on their target audiences**, notably communicating with associates and clients/users before drafting a press release.
- As much as possible, and as long as it does not further complexify the situation for the entity, **occupy media space**, before other actors (experts, influencers, service providers, clients, users, competitors) can speak in the entity's place.



FOCUS COMMUNICATING ON THE EXFILTRATION OF PERSONAL DATA

Data exfiltration refers to the theft or non-authorised transfer of data from a terminal or network, towards an outside device controlled by a malicious actor. Personal data is information which pertains to an identified or identifiable physical person who should therefore retain control over it. A physical person may be directly identified (for example: with a name and surname) or indirectly (for example: with a phone or licence plate number, credentials such as a social security number, a postal or email address, or even a voice or picture).

A cyberattack which enables data exfiltration is often followed by decryption blackmail, the publication of a sample, and the open-source reselling of the stolen data by the attacker.

Inherently visible, this type of attack generally has significant reputational repercussions and can cause serious concern amongst the entity's clients or users and partners. Furthermore, depending on the nature of the exfiltrated data, national and foreign media outlets may get heavily involved and social media may become flooded with comments. Crisis communication should therefore be adapted to this type of attack.

If an attacker publishes a data sample which they claim to belong to the entity, communication should comprise the following steps:



1st COMMUNICATION

Soon after the exfiltrated data has been published by the attacker, ANSSI recommends that the entity publicly state that it is aware of the potential incident affecting its systems. It should affirm that the qualification of the data is underway to confirm whether or not it actually belongs to the entity.



3rd COMMUNICATION

In cases where the rights and liberties of a physical person are being seriously threatened, the victim entity must individually inform each of the people involved of the theft of their personal data. **Article 34 of the General Data Protection Regulation (GDPR)** lists the conditions to meet. Also ensure that all affected individuals are able to verify the authenticity of the information received. Information should, by default, be shared on an individual basis to the people affected and, under derogation, may be communicated publicly. For more information on potential derogations, see article 34 of the GDPR.



2nd COMMUNICATION

If the exfiltrated data does not belong to the entity, a public statement needs to be made to refute the claim. If the exfiltrated data does belong to the entity, then the exfiltration and publication of personal data should be confirmed, including an apology for the damages caused to the affected individuals. Specify if the exfiltrated data belongs to the entity, or if it belongs to clients and was stored by the entity (in cases where the entity is a subcontractor). In the latter case, it is important for the entity to disclose what measures have been taken with regard to the relevant authorities: alerting ANSSI of the incident, filing a complaint with the police or gendarmerie's specialised services, initial and/or supplementary notification of the CNIL. To submit a notification, you may head to **notifications.cnil.fr/notifications**. Questions may also be addressed to **violations@cnil.fr**. It should also be specified that the data is undergoing precise qualification to determine its nature and that, if necessary, the individuals impacted by the exfiltration will be contacted.



REMEMBER

There is no one-size-fits-all approach to cyber crisis communication. The best-suited strategy is determined by the facts established, the situation in terms of communication, and the context. At the outset of a cyber crisis, communicators must present a communication stance to their executives: either proactive or reactive. The main objectives of crisis communication are to explain, inform, reassure, protect the entity's image and reputation, and promote a change in habits. Several target audiences must also be identified and addressed, both in-house (associates, managers, employee representatives, etc.) and externally (journalists, users, clients, shareholders, partners, authorities, etc.). Regarding the pacing, the duration of the incident's analysis and remediation does not align with media timing. In cases where reactive communication is favoured, the communicator must question the timing and relevance of a first communication. If a proactive communication stance is selected, the communicator must only and quickly communicate verified information, without committing to a specific recovery date, providing regular updates all the while and occupying media space whenever possible. It is also crucial to prioritise communications according to their target audiences, starting with informing associates and clients/users.

SECTION 6 DURING A CYBER CRISIS



FORMULATING KEY MESSAGES

1 FACTUAL AND TRUTHFUL INFORMATION

The topic of cybersecurity is now widely followed by a dedicated community. This community is made up of a broad range of influencers and discerning journalists seeking to better understand the tactics, techniques and procedures (TTPs) of attackers. It is highly active on social media, alerting users to incidents, discussing technical components, and commenting on the claims of attackers – and sometimes even on official communications. The cyber community takes note of events and may, even months later, call attention to the way in which they were handled, notably in terms of communication. In times of crisis, every communication is closely observed.

That is why communication must, first and foremost, be **truthful**. As with any other type of crisis communication, lying is highly inadvisable. Entities are not required to disclose everything, constantly and to everyone, but what information they do share must be truthful. The objective is to provide controlled transparency, for instance through regular situation reports. If an entity lies or refuses to communicate, its stakeholders may surmise that it has something to hide and draw their own conclusions – which could further amplify the ongoing media crisis.

If hypotheses are made at a given moment, they should be specified as such and spoken of in the conditional tense. For example: “At this stage, investigations do not suggest that any personal data has been compromised. Our teams are actively working on analyses to confirm this result.”

Communications must also be **factual**: value judgements should be avoided. The sophistication of the attack suffered should not be voluntarily or involuntarily minimised/exaggerated, as such deception would quickly be uncovered. It is therefore crucial for the entity to base its communications on the assessments made by its technical teams.

Lastly, it is recommended to have the strategic crisis unit review and approve the entity's messages.



The effort required to debunk falsehoods outweighs that which is initially invested in their production. During a cyber crisis however, any false information published either in-house or externally by associates, netizens, journalists, bots, etc. must imperatively be corrected.

2 TONE AND VOCABULARY USED

When formulating messages, particular attention should be paid to the vocabulary and tone used. The tone of communications should be pedagogical, reassuring, and may evolve alongside the crisis. Regarding the vocabulary to be employed:

- **Avoid overly alarming vocabulary:** the cyberattack itself induces enough stress; adding to it is unnecessary.
- **Tailor the technicality of messages to their target audiences:** cybersecurity is inherently technical and undergoes rapid technological developments. Accordingly, messages should be simplified as much as possible and, wherever complex words must be used, a definition should be provided. Conversely, the situation reports transmitted to Computer Security Incident Response Teams (CSIRTs) may employ the appropriate technical vocabulary. Any language specifically used within the entity should be avoided.

ANSSI's CyberDico may be used as a resource when drafting communication materials. It is available for free on the agency's website. This document lists, in alphabetical order, the various terms, phrases, and acronyms used in the field of cybersecurity. It provides their definition in both French and English and is regularly updated.



FOCUS ON EMPATHY AND HUMOUR

Challenging or facing a collective emotion with factual arguments alone is complicated. A message conveying both empathy and an apology is essential in the case of a cyberattack (particularly if there are individuals who have been directly impacted by the incident – in the case of data theft, for example). Using humour in an attempt to alleviate tensions is, however, inadvisable. Different people will perceive the situation in different ways, and humour may be interpreted as a sign that the incident is not being taken seriously – thereby contradicting the criticality and stress suffered by certain actors.

3 LANGUAGE ELEMENTS TAILORED TO THE SITUATION

The grid below can be a useful resource when developing communication content. It presents the following items:

- **A structure based on the FACET method** (F for Facts, A for Actions, C for Compassion, E for Engagement, and T for Transparency), to draft press releases, social media posts, and online news.
- **The questions most often asked during cyber crises.**
- **Advice for the formulation of proactive or reactive language elements.**

“In the thick of a cyber crisis, responsiveness is key to both internal and external communication. It is essential to quickly formulate and share clear and precise language elements, to acknowledge and explain the situation and to prevent rumours or a media frenzy.”

François Lecerf
Sales & Marketing Director,
LGM Group

FACTS

POTENTIAL QUESTIONS ASKED BY STAKEHOLDERS	ADVICE FOR THE FORMULATION OF PROACTIVE LANGUAGE ELEMENTS
What type of attack are we facing?	It is preferable to use the terms “cybersecurity incident” or “cyberattack” instead of “hacking”, as they tend to be less alarming. In cases where the attack fails, the incident may be referred to as an “attempted intrusion on the information system”. If the incident is caused by a technical issue and not a cyberattack, it is important to make this clear – using the term “technical failure”, for example.
What is the attack vector?	There exist different possible attack vectors: “compromised credentials”, “malware”, “phishing”, “DDoS”, “vulnerability exploits” or “zero-day vulnerabilities”, etc. Definitions for each of these terms may be found in ANSSI’s CyberDico. Both in-house and externally, the sharing of technical details pertaining to the way in which the attack occurred should be kept to a minimum. This information is not useful to your audiences and could fall into the hands of the attackers if they are still present on your information system (see Section 5).
What are the direct or indirect consequences of the cyberattack?	The consequences of the attack may be technical, organisational, or financial, on the structure, services or products provided by the entity. It is also crucial to specify whether or not lateralisation to the entity’s partners or clients has occurred.
Has data been exfiltrated?	In the case of potential data theft, refer to Section 5 .
When did the incident occur?	An approximate date for the start and/or detection of the incident may be provided (for example: “in the night from Friday to Saturday”, “this morning”). This can prove more difficult to do in the context of an attack aimed at espionage or sabotage, as the compromise is often detected several months or years after it occurs. In such cases, the detection date alone may be provided.
Is the attack still ongoing?	If the attack is over, the following answer may be provided: “following our investigations and the implementation of containment measures, we no longer detect any sign of an attacker on the information system.”

ACTIONS

POTENTIAL QUESTIONS ASKED BY STAKEHOLDERS	ADVICE FOR THE FORMULATION OF PROACTIVE LANGUAGE ELEMENTS
What actions have been undertaken?	It is fundamental to highlight: ▶ The actions undertaken to stop the cyberattack and to quickly restore the affected products or services (for example: isolation of the network, temporary interruption of certain services, disconnection of client/third party accesses to protect them, hardening of certain accesses, etc.) ▶ The establishment of a crisis unit. ▶ The services or products affected or unaffected by the cyberattack. ▶ Business continuity in a usual or degraded mode. ▶ Useful contacts in case of questions (for example: general email address or hotline).
Are you receiving support from ANSSI?	If such is the case, you may convey that: ▶ The French Cybersecurity Agency (ANSSI) has been made aware of the situation. ▶ The French Cybersecurity Agency (ANSSI) is assisting you as you handle this incident. This statement should be approved by ANSSI via the following email address: cert-fr@ssi.gouv.fr.
Are you receiving support from service providers?	It is recommended to let your audiences know if your entity is receiving support from private incident response providers or from CSIRTs (either sectoral, territorial, or ministerial), as it may provide some reassurance.

ACTIONS

Do associates, clients or users need to take measures? Are there best practices they might implement?	In your various communications, you may share practical guidelines with your associates, clients, or users: ▶ Specifically request that the telephone lines of your entity's IT services not be overloaded, as they will already be working towards the resolution of the incident. ▶ Provide technical or organisational guidelines to allow associates to continue their work. ▶ Share cybersecurity best practices, such as the renewal of passwords, the introduction of double-authentication, or the exercise of caution with regard to incoming emails.
What measures have been taken <i>vis-à-vis</i> the relevant authorities? In cases of personal data theft, has the CNIL been notified? Has a complaint been filed with the police or the gendarmerie's specialised services?	If such is the case, to demonstrate that your entity is capable of managing the cyber crisis, you may: ▶ Confirm in your communication that an initial and/or supplementary notification has been transmitted to the CNIL and, in this case, add that all affected individuals have been/will be informed (specifying the channel used, if it is known). ▶ Indicate that a complaint has been filed. The involvement of law enforcement will restrict your communications, as you will be unable to share certain specific details without the prior approval of the investigation service.

COMPASSION

POTENTIAL QUESTIONS ASKED BY STAKEHOLDERS	ADVICE FOR THE FORMULATION OF PROACTIVE LANGUAGE ELEMENTS
Would the entity like to address a message to the victims of the incident?	Showing compassion, it is important to address not only the direct victims of the crisis, but also any other individual who might consider themselves victims. The FACET method becomes CAFET (C for Compassion first, and Facts after Actions) whenever the crisis claims physical victims (wounded or dead). In such cases, compassion for the victims must come before all else.

ENGAGEMENT

POTENTIAL QUESTIONS ASKED BY STAKEHOLDERS	ADVICE FOR THE FORMULATION OF PROACTIVE LANGUAGE ELEMENTS
To what extent has the incident been addressed by the entity?	It is crucial to demonstrate that your entity has reacted quickly and efficiently, and that it is fully engaged in the management of the incident – with, for example, the establishment of a crisis unit. You may reaffirm that information system security and the protection of personal data is your top priority.
What measures will you be implementing in the future?	You may share what actions have already been undertaken to ensure the cybersecurity of your information system in recent years, as well as the lessons learned from this cyber crisis (for example: the introduction of an additional action plan or the release of a budget specifically dedicated to cybersecurity).

TRANSPARENCY

POTENTIAL QUESTIONS ASKED BY STAKEHOLDERS	ADVICE FOR THE FORMULATION OF PROACTIVE LANGUAGE ELEMENTS
How long is the situation expected to last? What next steps will need to be taken in order to resolve this crisis? When might we expect a return to normal or to optimal operation?	You must inform your audiences of the time required to complete the investigation and remediation process. Technical analyses are often long, remediation can take time, and surprises may arise. Do not commit to a specific recovery date at the beginning of the crisis; instead, provide visibility during the different stages of the investigation or of remediation (see Section 5). The following elements may be used: “The duration of our product and services’ unavailability, much like the time frame of our return to normal, remains to be determined.” “The service is momentarily unavailable.”
When will new information be shared?	To answer this question, you may state that investigations and remediation efforts are underway and that new information will be shared as soon as it is available. For example: “We will continue to keep our stakeholders informed as our investigations and remediation efforts progress.”
Who might we contact should we have any further questions?	Both within the entity and externally, the crisis unit and technical teams must be shielded from excessive solicitations with the implementation of a “buffer” which might allow them to fully focus on resolving the incident. You may, for instance, encourage audiences to use a contact form or general email address specifically created for the occasion, but this will entail managing large amounts of inquiries. A hotline may also be established to handle calls. Within the entity, it is recommended to establish a clear framework for media communications from the beginning of the crisis. Ask associates to transfer press inquiries to your press department, if they are contacted by journalists, to centralise the management of media relations.

ANSSI recommends that the following topics only be addressed reactively.

POTENTIAL QUESTIONS ASKED BY STAKEHOLDERS	ADVICE FOR THE FORMULATION OF PROACTIVE LANGUAGE ELEMENTS
Who is the attacker? What are their motives?	The French authorities differentiate the imputation of a given cyberattack (to an intrusion set or to a group of attackers) from its political attribution to an identified sponsor. ► Attackers may easily pretend to be something they are not, making false claims or planting false evidence to cover their tracks. The imputation of a cyberattack focuses primarily on the technical characterisation of the tools, techniques, and tactics used by the attacker, to discover their motives and methods, to connect them to other known cyberattacks, and to identify a group of attackers or a sponsor. The level of certainty accorded to this technical work varies, but it provides the basis for the possible decision of an attribution. ► The public attribution of a cyberattack is a political decision, taken at the highest level of government, intended to designate the group of attackers or sponsor (generally a state) responsible for the attack. That is precisely why, even if the media demands to know who is behind the cyberattack you have suffered, it is advisable not to publicly share information pertaining to the attacker. In this way you may avoid making mistakes, publicising the attacker, or giving the crisis a geopolitical dimension which could prove difficult to manage.

Have you received a ransom request and, if so, have you paid said ransom?

If the ransom request has already been made public, you may confirm it in your messages.

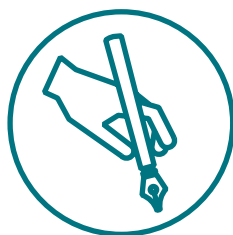
ANSSI recommends that ransoms never be paid. Indeed, the payment of a ransom does not guarantee that you will obtain the means of decrypting your data and, even if they are given to you, there is no guarantee that all of the encrypted files will be restored. It would not allow the restitution of the exfiltrated data, nor would it guarantee that it remains unpublished. Moreover, the payment of ransoms encourages cybercriminals to continue their activities, sustains this fraudulent system, and does not protect your entity from future cyber-criminal attacks.

If your entity is a public one, you may use the following answers: "In accordance with the doctrine of the French government and public administrations, no payments will be made to the cyber-criminals."

If your entity nonetheless decides to pay the ransom, it must, under the French Insurance Code⁷, file a complaint prior to making the payment in order to activate the clauses of your insurance contract. Keep in mind that even if it is done discreetly, quickly restoring your information system will arouse suspicions amongst cybersecurity specialists. The payment of a ransom will not get rid of the attacker's claim, and the attacker may even share the news of its payment.

Furthermore, it should be kept in mind that:

- **Each incident is unique.** As such, messages must be tailored to the situation and to their specific audiences (**see Section 5**).
- **Messages should evolve as the crisis progresses.**
- **The repetition of messages is a core principle** of communication and may be used without moderation.



REMEMBER

A pedagogical and reassuring tone should always be favoured in communication. Overly alarming terms should be avoided, and the technicality of the information shared should be adapted to its audiences. When using the FACET method (F for Facts, A for Actions, C for Compassion, E for Engagement, and T for Transparency), any information shared must be factual and true.

⁷ Code des assurances, Chapitre X: L'assurance des risques de cyberattaques (Article L12-10-1).

SECTION 7 DURING A CYBER CRISIS



MANAGING INTERNAL CRISIS COMMUNICATION

During a cyber crisis, internal communication is strategic. Associates must be kept informed, reassured, and aligned to prevent contradictory narratives, rumours, information leaks, or even panic.

If they remain accessible, continue using “traditional” internal communication tools:

→ **Team meeting or manager briefing**
(in person or remotely)

→ **Internal email or newsletter** (with a clear headline: “Important information – ongoing cyber incident »), which may include a message from the heads of the entity

→ **Intranet**

→ **Company social media account**

→ **Internal messaging platform**

→ **Dynamic display solutions on screens**

→ **Internal print newspaper**

→ **Paper displays on premises**
(break room, cafeteria, etc.)

If the cyber crisis restricts the entity's access to "traditional" tools, alternative solutions may be used to maintain communication with its associates:

→ Personal mobile phones and email addresses

→ Temporary instant messaging application

→ Private group on a general public social media platform

→ Pamphlets containing guidelines

→ Temporary email address (outside of the entity's information system) **created on a free messaging platform for private individuals**

→ Contact form on the intranet

→ "Pen and paper" mode

→ Regular mail

PRIORITIES FOR INTERNAL COMMUNICATION

Communication with internal audiences should be the entity's first priority (before external communication), as they are generally the first to be impacted by the incident. For example, a ransomware attack blocking access to the information system will often involve the display of a ransom request, or even of a countdown, on computer screens. This approach often causes turmoil and anxiety among the victim entity's teams and prevents associates from working. The goal is to ensure that associates do not learn about the ongoing crisis through the media or social media. Their working hours should also be taken into consideration, as well as any potential time zone differences for teams operating abroad, when defining the tempo of the entity's internal communications.

DISCRETION AND CONFIDENTIALITY

There is greater permeability between internal and external communication now than ever before, meaning that entities should be particularly careful with regard to the content shared with their associates (see Section 5). Internal communications often end up leaking externally.

It is also crucial to inform or remind associates of the way in which they are expected to engage with the media and with social media audiences.

→ **Media relations:** associates should be asked not to directly answer media inquiries and to instead transfer them to the entity's press department or, alternatively, to its executives. The goal is to centralise exchanges, to accurately assess the level of media pressure and, in so doing, to ensure a coherent and controlled response.

→ **Social media:** it is recommended to limit the number of individual communications addressing the incident, keeping in mind the reputational and legal risks faced (for example: the employment contract's confidentiality clause or the duty of confidentiality, discretion, or professional secrecy for civil servants).

PROXIMITY

Each level of the entity's hierarchy (managers, executives, etc.) may also be used to broadly distribute its messages to associates (see Section 5). Indeed, the proximity manager remains the essential link of the information chain.

CHANGING HABITS

Internal communication is an essential tool to achieve a change in cybersecurity habits. In the event of a cyberattack, it is common for internal communications to be addressed, detailing the implementation of multifactor authentication (MFA) or encouraging associates to change their passwords. The goal is to support change without generating internal panic or chaos.

“Well-managed crisis communication entails quickly and regularly informing associates of developments. The modalities of internal communication must therefore be defined ahead of time. This is especially important when anticipating a cyberattack which might cause the unavailability of certain internal communication tools.”

Clémence Picart

**Deputy Director of Dialogue and Communication
for the Nuclear Safety and Radiation Protection Body**



REMEMBER

To prevent rumours or panic, associates should be the first informed. Alternative means of communication should be used if “traditional” channels have been rendered unavailable. Keep in mind that internal communications may leak externally. Associates should be reminded of the way in which they are expected to engage with the media and social media audiences. Internal communication will also allow the entity to support associates in the implementation of more secure practices.

SECTION 8 DURING A CYBER CRISIS



MANAGING EXTERNAL CRISIS COMMUNICATION

MEDIA MONITORING

During a cyber crisis, media monitoring is an essential strategic tool which can be used to develop and adapt one's communication stance. Ahead of the crisis, this monitoring may facilitate the detection of faint signals – on social media, for example – which could indicate a technical incident (influencer post, an attacker's claim, etc.). In such cases, the communicator must notify all concerned stakeholders (entity heads, cyber/IT team, etc.).

At the outset of and during the cyber crisis, monitoring of traditional and social media must be established and maintained, whenever possible, by a dedicated person. It can also be useful to monitor any political addresses made or reactions had by associates internally (in collaboration with the internal communications officer). This monitoring makes it possible to better understand media reality and the pressure exerted on the entity, to steer its cyber crisis communication and assess its efficiency, and to identify recurring questions or criticisms among the entity's stakeholders regarding the incident and its management.

Given the massive amounts of information available, efficient monitoring requires a methodical approach.

1/ IDENTIFY THE RELEVANT INFORMATION TO MONITOR

To monitor audiences' general perception of the situation, the right keywords must be associated to the entity's monitoring tools. These must be broad enough to pick up as much relevant information as possible, but also specific enough to avoid excessive "media noise". The plural form of these words should also be included, along with their translation in different languages. For example:

- **The name of the entity**
- **The name of the entity's products or services**
- **The name of the entity's executives**
- **The terms** "cyberattack", "incident", "security incident", "data leak", "data theft", "sale of data", "data publication", "hacking", "ransom", "ransomware", "malware", "security breach", "DDoS", "denial of service", "phishing", "vulnerabilities", etc.

2/ IDENTIFY THE RELEVANT SOURCES TO MONITOR

Decide which media sources should be monitored:

- **Press agencies**
- **Written press** (national, regional, international media, industry-specific media, etc.) and its variants (print, web, social media accounts)
- **Online media** (general and thematic news sites, influential blogs, discussion forums, etc.)
- **Social media**, including the accounts of journalists, experts, opinion leaders, and influencers
- **Radio and television** (local, regional, national, and international)

3/ USE THE RELEVANT MONITORING TOOLS

There exist several different monitoring tools and services, available freely or at a cost:

- **Alert tools** immediately notify you by email when recently-published online content contains your keywords.
- **Automated tools** (content aggregators or professional monitoring platforms) can be used to gather all of the relevant content and automatically detect, in real time, new content published by the monitored sources which contain your keywords.
- **Specialised communication agencies** may also handle this monitoring in your stead.

4/ ANALYSE AND SHARE MONITORING RESULTS INTERNALLY

Once the monitoring tools have detected content associated with your keywords, said content must be carefully analysed through a global lens. To facilitate the analysis process, it is recommended to create dashboards (using graphs to quickly visualise the main emerging trends). During a cyber crisis, media monitoring will make it possible to analyse:

- **The number** of publications, mentions, likes, impressions, comments, shares etc.
- **The overall tone of messages**: positive (support, positive engagement), negative (criticisms, controversies, discontent), neutral (sharing of factual information).
- **Dominant narratives** (relaying of the entity's key messages, rumours, accusations, expectations of stakeholders, etc.).
- **The speed at which information spreads.**
- **Communications on social media** (by entity heads, associates, employee representatives, etc.).
- **The sources of messages** (journalists, influencers, political staff, etc.), and the spread of misinformation by bots.
- **The relaying of information and engagement sparked by the entity's crisis communication measures** (virality of a press release, engagement with publications pertaining to the incident, etc.).

Monitoring results may be shared internally through monitoring reports (which may also be automatically generated using various tools), email alerts, a newsletter, the intranet, etc.

Broadly used on social media, generative artificial intelligence (AI) chatbots have become opinion leaders and may make mention of your entity. During a cyber crisis, they may share false or only partially true information about the entity which users may accept as truthful. It is therefore crucial to take these new sources of information into account in the monitoring process.

DIGITAL COMMUNICATION

Social media and websites are essential tools which should be used responsibly in cyber crisis management.

All social media communications should be paused until a crisis communication strategy has been devised. Scheduled or sponsored posts should be removed from social media management tools. Any news shared on the entity's website during the incident must be relevant.

Information (and misinformation) travels fast of social media, and the public expects immediate answers. Without rushing, the entity must ensure the **relevance of the first post published on its social media platforms** following the start of the crisis, making sure that it resonates with its external audiences. First impressions are incredibly important!

Social media platforms can be used to both share official information and maintain dialogue with the public. **The comments and publications made by users should therefore be managed wisely.** Responses may be given to legitimate criticism using reactive language elements (which should be tailored to the entity's usual editorial line) or, if necessary, they may be redirected towards a private channel. It is recommended not to conceal negative comments to avoid overreactions from the

original posters, and it is advised not to answer the “trolls” present on certain social media platforms. Indeed, these individuals will seek to discredit the entity by provoking it into making a mistake.

It is preferable to **tailor messages to each one of the platforms used, with each publication being neatly formatted** (photo, video, image, text, etc.). Emojis should be used and any sensitive information shown in the pictures posted should be concealed. It is also crucial to use a relevant hashtag which will often be used to refer to the ongoing incident. Particular attention should be paid to the regularity and timing of publications to ensure that they are seen by large audiences. The number of different formats should however be limited to ensure that communications remain cohesive.

Associates (see Section 7) should not be permitted to fuel the media crisis with spontaneous and clumsy declarations on social media.

Where appropriate, it is recommended to use the entity’s employee advocacy program to call on key associates, “ambassadors”, to share predetermined approved information via their social media accounts. This approach allows for a more embodied and amplified form of communication.

The **« News » section of the entity’s website may also be used** to share information. If the incident has rendered the website inaccessible, a temporary website presenting essential information pertaining to the entity may be set up during the crisis. If this approach proves to be overly time-consuming, a simple banner may be added to the website’s home page, informing users that any information pertaining to the ongoing cyber crisis may be found on the entity’s social media accounts.

For a more transparent approach to social media communication, it can be useful to **share the “behind the scenes” of crisis management**. Publications (photos, etc.) may be made portraying associates “in action”, implementing measures to ensure service continuity.

Keep in mind that **a publication may become viral and garner a lot of reactions**. This rapid and unpredictable dissemination may be positive or, on the contrary, it may give rise to bad buzz which could sully the image of the entity or its executives. Such phenomena often begin on social media and can sometimes spread to other media.

The entity's press conference may also be broadcast live on social media to reach a broader community beyond the journalists physically present.

Social media (and LinkedIn more particularly) allow entity heads, during a crisis, to simultaneously and directly (without intermediaries) share messages with different stakeholders (associates, clients, users, investigators, media, etc.). **The word of the entity head, in their name, grants the message a more human dimension and may reassure audiences by proving that the crisis is being managed at the highest level.** Publications by the entity head may also be shared on the entity's social media accounts.

MEDIA RELATIONS

The nature of the interactions had with journalists during a cyber crisis will significantly impact the perception that audiences (clients/users, service providers, financial partners, authorities, associates, citizens, etc.) have of the situation. A relationship of trust must be established with journalists, based on the respect of their constraints, on transparency, and on the regularity of the information shared. Keep in mind that certain key parameters cannot be controlled:

- Each journalist is free to make their own editorial choices (title, angle, etc.) and they may decide, alongside their managers, to use – or not use – the information shared.
- Editorial priorities may change at any given moment, depending on current events, and it is not possible to decide on the time of publication.

In a context where media defiance, infobesity, and AI are on the rise, media relations can, through the provision of reliable and verified information to journalists, play a central role in countering the spread of misinformation.

It is therefore crucial to work closely alongside media relations teams to prepare content to share with journalists:

- **A press release** (see dedicated “focus”)
- **An interview** (see dedicated “focus”)
- **A press conference** (see dedicated “focus”)

First and foremost, if the cyberattack suffered by the entity is visible, all press-related endeavours scheduled before the incident should be suspended. The ongoing cyber crisis is going to be the only subject in which journalists are bound to show interest; as such, it would be inappropriate to proceed with communications unrelated to the incident.

In the event of an incident, the entity’s usual journalist contacts may reach out, as well as media outlets specialised in IT and general media journalists working in cybersecurity/tech services. ANSSI generally does not communicate in the victim’s stead; instead, press inquiries pertaining to cyber incidents are automatically transferred to the (potential!) victim.

Each person’s role within the cyber crisis communication framework must be clearly defined, shared, and understood by all. To ensure that the entity maintains good command over its messages, it is recommended to limit the number of interlocutors interacting with the media and to prepare, ahead of time, for these interactions. During a crisis, the head of the entity naturally becomes the favoured spokesperson: their statement emphasises the entity’s firm commitment and enhances the credibility of the messages shared. However, other spokespersons may be designated and used gradually so that the entity head may only be called upon when the crisis is at its peak.



FOCUS

AI AS AN OFTEN-USEFUL TOOL IN TIMES OF CRISIS

Note that, at the very least, the spelling-based proofreading of content before its publication can be carried out by generative AI. With a relevant prompt, AI may also be used to produce crisis communication content (press releases, social media posts, etc.). Sensitive or confidential data should however never be shared with this type of tool, and any content produced by AI should be critically reviewed. The Government Information Service (SIG) has formulated guidelines for the use of artificial intelligence by the government's communicators, in line with other common rule sets (state branding, accessibility charter, state design system). This document may be found on the *Info.gouv.fr* website.

1/ THE PRESS RELEASE

Press releases, when formulated well, can be useful tools during cyber crises. However, if they are overly complicated and difficult to understand or too concise and not shared with the right audiences, they can become counter-productive.

→ BEFORE STARTING

It is crucial for the press release to have a clear objective. Before it is drafted, the following questions should be considered:

WHO IS IT BEING WRITTEN FOR?

When communicating on a cyber crisis, journalists specialised in cybersecurity/tech (and their readers) and general journalists (and their readers) will both be addressed.

WHY IS IT ADDRESSING THIS TOPIC?

Journalists receive dozens of press releases daily; yours must be efficient. Keep in mind that the press release is not being written for your entity, but rather for the journalists to which it is addressed.

WHAT IS IT ABOUT?

The press release should answer six fundamental questions, following the 6W method:

► **Who?**

Who is impacted?
Who is responsible?

► **What?**

What is the event?
What happened?

► **When?**

When did this happen?
When will this happen?

► **Where?**

Where did this happen?

► **Why?**

Why is this happening?
What are the causes or motives?

► **How?**

How did this happen?
How should this be handled?

→ CONTENT OF THE PRESS RELEASE

INTRODUCTION OF THE PRESS RELEASE

The entity's logo should be included, along with a place and date, especially if other press releases are going to be published in the days that follow.

TITLE

This is the most important part of the press release:

- ▶ Formulate it last (once the content has been written, to ensure that it reflects the rest of the press release).
 - ▶ It must convey enough information to ensure that the person receiving the press release quickly understands what it is about, following the following structure: Subject > Action > Topic.
 - ▶ It should be concise (no more than two lines).
- When the press release is cited by the media, its title is likely to be "copied and pasted" and shared on social media.

HOOK

In one or two sentences, the aforementioned 6Ws should be answered.

- ▶ Make it simple and concrete.
- ▶ Do not attempt to provide further details at this stage.

MAIN BODY

It is recommended to use the FACET method (Facts, Actions, Compassion, Engagement, Transparency) when completing the body of the press release ([see Section 6](#)).

Additionally:

- ▶ Check that the press release provides an answer to each one of the 6Ws.
- ▶ Write in third person, as a journalist would in a news article.
- ▶ A quotation (preferably by the entity's executives) may be used to convey an important message.
- ▶ Avoid using jargon as the press release must be accessible to all audiences ([see Section 6](#)).

CONCLUSION

- ▶ Briefly include additional information on the entity; the "about" section.
- ▶ Name the person(s) to contact for more information (the entity's press officer or media relations agency).

2/ THE PRESS CONFERENCE

This approach can be useful as a **single statement can convey many messages to a large number of journalists**. Press conferences also provide an opportunity for journalists to converse with spokespersons during the question-and-answer session.

This approach can, however, also be perilous: the entity must be able to answer the many questions that journalists will inevitably have regarding the cyber crisis or any other topical issue.

When scheduling a press conference, it is imperative **to choose a time and place which will fit into the time tables of journalists, giving mind to the entity's own constraints all the while**. A list of the different media to invite should also be drawn up.

Journalists should be notified as early as possible, and invitations should briefly outline the objective of the press conference and provide any important details such as the date, time, and place. Keep in mind that the press conference may be broadcast live on a television channel or online, and that this would only enhance its impact.

During a cyber crisis, the objective of the press conference is generally to assess the situation. It is typically broken down into 3 main parts:

- **Addresses by one or several spokespersons.**
- **A question-and-answer session** with journalists.
- **Interviews with spokespersons** for broadcast media at the end of the press conference.

Additional informal discussions with certain journalists may also be scheduled.

Note that press conferences should be exceptional occurrences. This is a time-consuming format that is no longer favoured by journalists unless it is rare and considered to be worth the trip.

3/ THE INTERVIEW

The interview should be conducted in writing, in audio (in a studio, by phone), or in video (on set, duplex), recorded or broadcast live.

The journalist will be expecting:

- Initial or new information pertaining to the cyber crisis.
- A concrete description of events (**see Section 6**) and numbers.
- A spokesperson who expresses themselves clearly, providing specifics, and who uses effective punch lines.

Note that making an exclusive statement to a major press agency, such as the France-Presse Agency (AFP), the Associated Press (AP), Reuters, or Bloomberg, may be an effective strategic decision depending on the nature of the entity's activities and on its national and international interests. The press agency would then, via a dispatch, share the entity's messages with the rest of the national and international media. This approach has many benefits:

- **Controlling the narrative:** by eliminating direct sources, the risks of distortion and of the multiplication of interpretations are reduced.
- **Gaining time:** limiting interactions to a single agency prevents the entity from having to engage with a number of different journalists.
- **Ensuring broad and homogeneous media coverage:** when it is cited by different newsrooms, the dispatch facilitates the rapid, unified broadcasting of information.

“In 2025, after having suffered a cyberattack on its data bases, the city immediately informed users. Due to its exposure to industrial risks, the city was accustomed to crisis management and implemented its usual methods, sharing specific information pertaining to the facts and known consequences of the attack.”

Romain Boix
Chief of Staff,
Pont-de-Claix



REMEMBER

In the event of a cyber crisis, media monitoring is essential: monitor mentions, the tone of conversations, and the dominant narratives to adapt your communication in real-time. The entity's social media accounts and website are strategic channels: scheduled posts should be postponed and each message should be tailored to its specific platform. Concerning media relations, inquiries should be centralised via the entity's press department and a press release should be prepared following the FACET method and the 6W rule. Inquiries from your usual media contacts as well as from journalists specialised in cybersecurity/tech are to be expected. ANSSI does not communicate in the victim's stead; instead, press inquiries are systematically transferred to the concerned entity.

AFTER A CYBER CRISIS



When the cyber crisis comes to an end, teams may be tempted to quickly resume their activities. However, this period of transition towards the entity’s full recovery is the best time to perform a number of communication activities. The following pages provide practical guidelines detailing these activities.

Section 9 : Thanking associates and reviewing experience feedback ... 71
Section 10: Sharing experience feedback and raising awareness amongst associates 73

SECTION 9 AFTER A CYBER CRISIS



THANKING ASSOCIATES AND REVIEWING EXPERIENCE FEEDBACK

THANKING ASSOCIATES

It is essential to thank both the entity's external and internal stakeholders for their collaboration on the resolution of the cyber crisis. The message addressed to internal associates should acknowledge their collective effort, thanking them for their professionalism and commitment during the incident, and should ideally be signed by the entity's executives. It may also contain a reminder of the best cybersecurity practices to adopt and announce the start of an experience feedback reviewing process.

REVIEWING EXPERIENCE FEEDBACK

In the aftermath of the cyber crisis, it is necessary to go over the communication measures implemented, capitalising on these experiences and figuring out what could stand to be improved. Reviewing experience feedback makes it possible to improve the resilience of the entity's communications team, identifying highlights and potential areas for improvement if any deficiencies are noted. It also provides an opportunity for certain crisis communication measures identified as effective to be perpetuated. The feedback review should take place following the end of the cyber crisis and should not be perceived as an audit but rather as a capitalisation measure.

It should comprise two phases:

- An **"immediate" experience feedback review**, in the form of interviews or information gathering workshops.
- A **"retrospective" experience feedback review**, presenting a summary of the observations made, recommendations, and the associated action plan.



REMEMBER

It is imperative to send thank-you messages to the entity's various internal stakeholders and to perform an experience feedback review to go over the communication measures implemented during the cyber crisis.

SECTION 10 AFTER A CYBER CRISIS



SHARING EXPERIENCE FEEDBACK AND RAISING AWARENESS AMONGST ASSOCIATES

SHARING EXPERIENCE FEEDBACK

Public testimony may inspire and enlighten other actors to the risks and measures to implement in order to prevent cyberattacks. By sharing experience feedback, the entity effectively illustrates how this challenge was met and helps to strengthen cybersecurity in its field. Moreover, a well-managed cyber crisis can be used as an example. This will also demonstrate that the entity is capable of learning from the difficulties faced and of making security its priority.

”During and after the cyber crisis, we decided to also share our experiences with the rest of our ecosystem in order to alert our counterparts and allow them to prevent this type of attack (password spraying).”

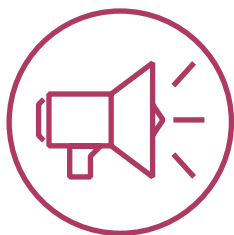
Nadège Aroumougom
Strategy, Marketing, and Communications Director,
Alptis Assurances

RAISING AWARENESS AMONGST ASSOCIATES

Once under control, a cyber crisis represents an opportunity for teams to channel new energy into cybersecurity. It may be a chance to prepare an internal awareness-raising campaign, alongside the cyber/IT team, sharing the cyber best practices to adopt. Depending on the entity's specific characteristics (size, workforce, sensitivity of activities, level of awareness of associates, available means of communication, etc.), different actions may be considered:

- Information meetings
- Poster campaigns
- Distribution of best practice guides
- Quizzes
- Phishing test campaign

The [Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr) website provides access to resources and ideas to effectively conduct internal awareness-raising campaigns.



REMEMBER

Public testimony may inspire and enlighten other actors to the risks and measures to implement in order to prevent cyberattacks. A cyberattack also represents an opportunity for associates to strengthen their commitment to the implementation of cyber best practices.

CHECKLIST

BEFORE A CYBER CRISIS

- ☐ Initiate a meeting between your communications team and cyber/IT teams to promote greater mutual understanding of their respective priorities, challenges, and vocabulary.
- ☐ Develop different communication strategies based on plausible cyber crisis scenarios (DDoS, ransomware, defacement, etc.).
- ☐ Assemble a toolbox dedicated to cyber crisis communication.
- ☐ Take part in a cyber crisis exercise to test the resilience of your communications team and tools in the face of a cyberattack.
- ☐ Media train your spokespersons to improve their reflexes.

DURING A CYBER CRISIS

- ☐ Establish a crisis-specific organisational framework for your communications team, with the distribution of roles (coordination, perception, and reaction) and missions.
- ☐ Take stock of the facts, of the situation in terms of communication, and of the context.
- ☐ Present your executives with a communication stance to adopt: proactive or reactive.
- ☐ Define your primary communication objectives (to explain, inform, reassure, preserve the entity's image and reputation, promote a change in habits).
- ☐ Identify and address your internal (associates, managers, employee representatives, etc.) and external (journalists, users, clients, shareholders, partners, authorities, etc.) target audiences.
- ☐ In cases where a reactive approach to communication is selected, question the timing and relevance of an initial communication.

DURING A CYBER CRISIS



In cases where a proactive approach to communication is selected, quickly communicate verified information only, do not commit to a specific recovery date, regularly inform your audiences and, wherever possible, occupy media space.



Prioritise communications depending on your target audiences and start with informing your associates and clients/users.



Use a reassuring, pedagogical tone.



Avoid overly alarming terms and adapt the technicality of the information shared to its target audience.



Communicate factual and truthful information.



Use alternate means of internal communication if your “traditional” channels are unavailable.



Keep in mind that your internal communications run the risk of being leaked externally, and remind your associates of the way in which they are expected to engage with the media or social media audiences.



Monitor mentions, the tone of conversations, and the dominant narratives on social and traditional media to adapt your communication in real-time.



Suspend scheduled social media posts and tailor each message to its specific platform.



Centralise press inquiries via your press department and prepare a press release following the FACET method and the 6W rule.

AFTER A CYBER CRISIS



Send thank-you messages to your internal stakeholders.



Perform an experience feedback review of the communication measures implemented during the cyber crisis.



Deliver a public testimony to inspire and enlighten other actors on the risks and measures to implement to prevent cyberattacks.



Raise awareness amongst your associates on the cyber best practices to adopt.

RESOURCES

FIND ALL OF ANSSI'S BEST PRACTICE GUIDES ON
messervices.cyber.gouv.fr

Remediation series



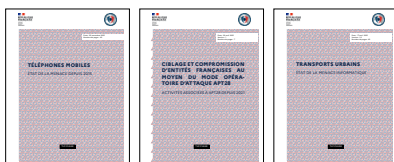
Other guides in the Cyber Crisis Management series



Threat and incident reports



Annual Cyber Threat Overviews



CyberDico

ANSSI's CyberDico lists, in alphabetical order, the various terms, phrases, and acronyms commonly used in the field of cybersecurity. It provides translations and French definitions for each of these.

www.cyber.gouv.fr/cyberdico

You may also find news bulletins, alerts and safety notices, guidelines, and industry-specific cyber threat overviews on the CERT-FR's website www.cert.ssi.gouv.fr

Version 2.0 – Septembre 2026
Licence ouverte/Open Licence (Etalab — V2)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI — 51 boulevard de la Tour-Maubourg — 75700 PARIS 07 SP
www.cyber.gouv.fr

