**Le nouveau plan Vigipirate**

La protection du territoire national, de la population qui y vit et de ses ressortissants à l’étranger est une responsabilité essentielle de l’Etat. Il lui appartient également de garantir la continuité des fonctions essentielles de la Nation, notamment celles qui relèvent du fonctionnement de l’Etat et de la vie de la population.

Le plan Vigipirate consiste en un dispositif permanent de vigilance, de prévention et de protection face à la menace terroriste ou en réaction à une attaque. Il couvre l’ensemble des activités du pays et associe tous les acteurs de la Nation. En ce sens, il constitue un instrument majeur concourant à la sécurité nationale, définit des stratégies et des objectifs de sécurité et propose des mesures opérationnelles pour l’ensemble des acteurs concernés.

1. **Les caractéristiques du nouveau plan Vigipirate**

S’il a, comme le précédent, pour objectifs de développer et maintenir une culture de vigilance de l’ensemble des acteurs de la Nation afin de prévenir ou de déceler le plus en amont possible toute menace d’action terroriste, d’organiser un dispositif national de préparation des moyens de protection et de réponse, de permettre une réaction rapide et coordonnée en cas d’action terroriste, le nouveau plan approuvé par le Premier ministre présente trois caractéristiques.

**1° Il est en grande partie public**, afin d’informer la population des mesures de protection et de vigilance qui la concernent, et à mieux mobiliser l’ensemble des acteurs du plan. Un document classifié est cependant destiné aux pouvoirs publics et aux opérateurs d’importance vitale, comprenant toutes les précisions nécessaires à sa mise en œuvre et le détail de mesures qui ne concernent pas directement les ministères de l’éducation nationale et de l’enseignement supérieur et de la recherche.

**2° Il est simplifié** par la référence à deux niveaux d’alerte au lieu de cinq (représentés précédemment par des couleurs), visualisés par un logo affiché dans les lieux publics :

* la **vigilance** correspond à la posture permanente de sécurité. Elle se traduit par la mise en œuvre d’un socle de mesures permanentes d’intensité variable selon la vulnérabilité des sites ; cette vigilance peut être **renforcée** par l’addition de mesures plus contraignantes mais temporaires pour faire face à une augmentation de la menace terroriste ou de certaines vulnérabilités ;
* l**’alerte attentat** s’applique soit à un contexte de péril imminent, soit à une situation où une ou plusieurs actions terroristes sont commises sur le territoire national : des mesures exceptionnelles et temporaires, **éventuellement très contraignantes** sont alors à prendre.

**3° Il adopte une approche par des** **objectifs de sécurité propres à chaque domaine**, permettant de choisir au sein d’un répertoire les mesures de vigilance et de protection les plus adaptées au niveau de menace, dans une logique de proportionnalité afin de réduire les vulnérabilités sans induire de contraintes excessives sur la vie économique et sociale de la Nation.

Ainsi les mesures du plan sont classées et numérotées, dans chacun des 12 domaines d’activité, en fonction de l’objectif de sécurité qu’elles visent dans ce domaine (premier chiffre) et en fonction du degré de contrainte envisageable dans les modalités de leur application (deuxième chiffre). Ce degré de contrainte peut varier en fonction du moment ou de la sensibilité du site auquel s’applique cette mesure. Ce degré de contrainte peut ainsi être affiné et modulé dans le cadre du niveau général d’alerte en vigueur.

**4) Chaque ministère est ainsi appelé à décliner et à diffuser les instructions** nécessaires en direction de ses services déconcentrés et de ses établissements ou opérateurs dont il a la tutelle, des **instructions étant également transmises par le ministère de l’intérieur aux préfets**, qui en informent les collectivités territoriales de leur département, s’assurent de la bonne information des opérateurs et veillent à la cohérence des mesures mises en œuvre par les différents acteurs.

C’est pourquoi les recteurs veilleront, suite aux instructions qu’ils reçoivent du ministère (HFDS), à ce que ces instructions, déclinées par leurs soins auprès des services académiques et des établissements, soient communiquées aussi aux préfets des départements.

Le grand public est pour sa part informé de l’évolution de la menace terroriste et des changements de posture Vigipirate par les déclarations du Premier ministre et des ministres concernés, mais également au travers du site internet du gouvernement **www.risques.gouv.fr** qui donne les informations les plus récentes et renvoie à une base documentaire complète sur le plan Vigipirate.

Les niveaux Vigipirate sont exprimés dans l’espace public au travers d’une signalétique associée à un triangle de couleur rouge pour signaler le danger. En situation d’alerte attentat, la mention « alerte attentat » est ajoutée.

1. **Principaux objectifs de sécurité et mesures pour l’éducation nationale, l’enseignement supérieur et la recherche**

Le plan décrit au sein de chacun de ses 12 domaines:

* + - les **objectifs** de sécurité propres au domaine,
		- les mesures permanentes de vigilance et de protection à mettre en œuvre en toutes circonstances, et qui constituent le **socle permanent de vigilance**, de prévention et de protection ;
		- les mesures **additionnelles** susceptibles d’être mises en œuvre en fonction de l’évaluation de la menace ou de vulnérabilités particulières.

Les ministères de l’’éducation nationale et de l’enseignement supérieur et de la recherche sont impliqués principalement dans la mise en œuvre de mesures des domaines de l’alerte (ALR), de la sécurité des établissements recevant du public et des bâtiments (BAT) et de la cybersécurité (CYB) qui, au demeurant, concourent à la sécurisation générale des établissements scolaires vis-à-vis de tout type d’agression.

Ils sont concernés aussi, mais, plus exceptionnellement, par les domaines des grands rassemblements (RSB) et de la sécurité à l’étranger (EXT) en raison notamment des voyages scolaires, de la mobilité étudiante et des déplacements des chercheurs.

Les tableaux ci-dessous précisent les objectifs et les mesures à appliquer pour les deux ministères

1. **Alerter et intervenir**

L’alerte vise à transmettre une information dans l’urgence à tous les acteurs concernés afin de mobiliser immédiatement les moyens d’intervention et d’adapter les mesures de protection. Ce domaine d’action mobilise des moyens divers et complémentaires qui doivent être entretenus, être disponibles en permanence et pouvoir fonctionner en situation dégradée.

L’alerte en cas de menace imminente d’attentat ou d’attentat réalisé est **d’abord assurée par** **l’Etat, ses administrations et ses services**. Elle est ensuite relayée par d’autres acteurs : les collectivités territoriales et les opérateurs. Les responsables de chaque secteur d’activité doivent également être en mesure de déclencher une alerte selon la nature de la crise. On notera à cet égard que l’alerte au public peut se faire par sirène du réseau national d’alerte, médias et tout autre vecteur.

|  |
| --- |
| **Objectifs et mesures:** **1 Alerter et communiquer*** + - Disposer d’une chaîne d’alerte et d’information la plus large possible, la vérifier et la tester régulièrement (ALR 10.01) : veiller à la réalité des permanences, à la disposition des répertoires d’urgence, au bon état des moyens de communication ;
		- En cas de crise être en mesure d’activer une cellule de crise (ALR 11-01) ;

**2 Mobiliser et intervenir*** + - Elaborer et mettre à jour un plan de continuité d’activité (ALR 20.01) pour les services et les établissements.
 |

1. **Protéger les installations et bâtiments (lieux circonscrits par une enceinte)**

Le domaine des installations et bâtiments concerne l’ensemble des édifices qui peuvent constituer des cibles potentielles, soit en raison de leur valeur symbolique, économique, politique, soit en raison du public qu’ils accueillent. Il est donc commun à de très nombreux secteurs et établissements recevant du public comme les administrations, les entreprises, les commerces, les lieux touristiques, les lieux de culte, **les établissements d’enseignement** incluant ceux de l’enseignement supérieur et de la recherche **…**

L’architecture de ces derniers permet rarement d’empêcher physiquement toute intrusion. De plus la concentration des flux d’entrée et de sorties est peu compatible avec des dispositifs tels que des portiques de détection ou des sas de sécurité.

C’est pourquoi, en tenant compte des diagnostics de sécurité, une attention doit être portée à la surveillance à l’entrée et à l’intérieur, ainsi qu’à la coordination avec les services de sécurité publique pour ce qui concerne les abords et les collectivités de rattachement pour ce qui concerne les équipements des établissements scolaires. A cet égard la règlementation applicable aux établissements recevant du public (ERP) concourt à leur protection contre la menace terroriste, en permettant de limiter les risques d’incendie, d’alerter les occupants en cas de danger, de faciliter l’évacuation, d’alerter les secours et de faciliter leur intervention.

Dans le cadre de cette coordination, le chef d’établissement tant pour l’éducation que pour l’enseignement supérieur et la recherche prend toute disposition de nature à assurer la sécurité des personnes et des biens. Cependant l’adhésion des personnels, des élèves et de leurs parents ainsi que des étudiants aux dispositions de sécurité, qui devraient figurer dans les règlements intérieurs, est nécessaire.

|  |
| --- |
| **Objectifs :** surveiller, contrôler et filtrer les entrées et la circulation dans les bâtiments et enceintes des établissements de manière à identifier toute personne ou objet suspect et être en mesure soit d’empêcher l’accès, soit de donner l'alerte et mettre la population à l’abri en cas d'intrusion ou de flagrant délit..**Mesures :*** + - adapter la sûreté des accès en surveillant les accès des personnes, des véhicules et objets entrant dans l’établissement (mesures (BAT 20-01, 21-01, 22-01, 23-01) ;
		- adapter la sûreté interne en réglementant l’accès aux zones internes sensibles, en surveillant la circulation interne (mesures BAT 30-01, 30-02, 31-01) ;
		- dans les ***sites les plus sensibles***, ou dans l’ensemble des établissements en cas de situation correspondant à un niveau ***d’alerte renforcée***, contrôler les entrées des personnes, des véhicules ou des objets entrant (dont le courrier) par des inspections visuelles ou fouilles avec le consentement des intéressés
		- En cas de péril imminent, dans un contexte ***d’alerte attentat*** confiner les élèves, les étudiants ou si cela s’avère nécessaire, fermer préventivement l’établissement en liaison avec l’autorité académique et préfectorale ou le maire s’agissant des écoles.

**Recommandations permanentes de sécurité*** Contrôler les clôtures et systèmes d’alarme ou de surveillance, vérifier les dispositifs d’évacuation rapide ;
* Signaler aux autorités ou aux responsables de site tout élément suspect (bagage abandonné, véhicule ou comportement suspect, lettre ou colis suspect) y compris aux abords de l’établissement (cf fiche réflexe jointe) ; ne pas accepter de prendre en compte un bagage ou un colis ;
* Se conformer aux consignes permanentes ou ponctuelles de sécurité émanant de l’autorité académique ou du préfet.
 |

1. **Assurer la cybersécurité**

Les systèmes informatiques font l’objet d’intrusions et d’attaques de toute nature et doivent être soumis à des règles permanentes de sécurité. Celles-ci s’appliquent a fortiori aux attaques malveillantes qui peuvent non seulement affecter la confidentialité et l’intégrité des données personnelles, sensibles pour les deux ministères, mais encore la disponibilité des systèmes d’information dont dépendent des services essentiels.

C’est pourquoi un dispositif de cybersécurité spécifique au plan Vigipirate est prévu. Il concerne les acteurs nationaux comme l’agence nationale de la sécurité des systèmes d’information (ANSSI), mais aussi les opérateurs et les administrations dans leur ensemble en tant que responsables de systèmes d’information de l’État (il est rappelé que les recteurs sont « autorités qualifiées », ou personnes responsables de la sécurité des systèmes d’information au niveau des rectorats). Il concerne aussi les collectivités territoriales, les citoyens qui, chaque jour, dans leur vie professionnelle ou privée, ont un rapport avec les systèmes informatiques.

|  |
| --- |
| **Objectifs :** Renforcer la vigilance et la protection sur les systèmes d’information critiques ou essentiels contre des menaces identifiées afin d’assurer un niveau de disponibilité suffisant des systèmes d’information ; maîtriser les risques, gérer les incidents, évaluer le niveau de sécurité.**Mesures :*** + - Renforcer la protection contre les intrusions dans les systèmes d'information.

Cette mesure permet de détecter les signes préliminaires à des opérations de sabotage et d’être en mesure d’identifier et de traiter sans délai les intrusions ou tentatives d’intrusion dans les systèmes et d’en rendre compte (CYB 42.01 ; 43.01)* + - Renforcer la protection contre les attaques en déni de service.

Cette mesure permet de s’opposer à des opérations de sabotage non destructrices (CYB 42.02 ; 43.02)* + - Renforcer la protection contre une menace sectorielle. Cette mesure permet notamment de s'opposer à des opérations de sabotage destructrices (CYB 42.03 ; 43.03)

Les recteurs de même que les présidents ou directeurs des établissements d’enseignement supérieur et de recherche seront destinataires, par leurs RSSI, des actions détaillées permettant d’atteindre les objectifs de SSI. La plupart procède du référentiel général de sécurité des systèmes d’information et de la politique interministérielle de sécurité qui sera à mettre progressivement en œuvre pour élever le niveau général de sécurité. Enfin il convient d’appliquer en permanence les dix règles d’hygiène informatique suivantes.* + 1. Choisir des mots de passe robustes.
	+ 2. Mettre à jour vos systèmes d’exploitation et vos logiciels.
	+ 3. Utiliser les droits d’administrateur avec modération.
	+ 4. Effectuer des sauvegardes régulières.
	+ 5. Sécuriser votre point d’accès Wi-Fi.
	+ 6. Etre prudent lors de l’ouverture d’un courriel.
	+ 7. Télécharger les programmes sur les sites de leurs éditeurs.
	+ 8. Etre vigilant avant d’effectuer un paiement sur internet.
	+ 9. Séparer les usages personnels des usages professionnels.
	+ 10. Prendre soin de ses informations personnelles et de son identité numérique.

Toutes les recommandations essentielles à destination des citoyens sont disponibles sur le portail de la sécurité informatique : [www.securite-informatique.gouv.fr](http://www.securite-informatique.gouv.fr/) |

1. **Protéger les rassemblements de masse**

La protection des rassemblements, qu’il s’agisse de réunions ou manifestations publiques à caractère éducatif, récréatif, sportif ou culturel, concerne plusieurs types d’acteurs : les organisateurs, l’autorité administrative (maires, préfets), les forces de l’ordre (police, gendarmerie, forces mobiles, polices municipales). Les organisateurs sont responsables de la sécurité générale du rassemblement.

Il conviendra pour eux de se conformer aux exigences de l’autorité administrative responsable de l’ordre public (maire ou préfet en fonction de l’importance du rassemblement) qui peut imposer des mesures particulières afin de renforcer le dispositif de surveillance et de contrôle (mesure RSB 10.01, 11.01, 12.02, 13.02).

Au-delà des rassemblements de masse, il convient de veiller, en ce qui concerne les établissements scolaires, à ce que les mesures réglementant le stationnement à proximité de leurs accès où généralement se regroupent des élèves soient bien appliquées, en liaison avec les services de police et les municipalités.

Enfin, concernant les transports scolaires, il convient de s’assurer en liaison avec les collectivités compétentes vis-à-vis des transporteurs que les mesures de sécurité son effectives. Les voyages scolaires organisés entrent dans ce cadre général de la sécurisation des transports publics et des lieux de visite ou de rassemblement. En ce qui concerne les voyages à l’étranger, il convient d’observer les mesures du domaine « EXT » relatif à la protection des ressortissants français à l’étranger.

.

1. **la protection des ressortissants français à l’étranger**

Cela concerne les voyages scolaires, les déplacements des étudiants et des enseignants chercheurs ou des missions pour lesquels il convient de suivre les recommandations du ministère des affaires étrangères telles qu’elles sont consultables en permanence sur le site <http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/> et de s’inscrire sur le portail d’enregistrement des voyages à l’étranger « Ariane ».

Une circulaire de l’éducation nationale définit les responsabilités en matière d’organisation de voyages et en cas de dommages résultant de leur empêchement.

Enfin il est recommandé aux services académiques d’être informés des voyages scolaires à l’étranger organisés par les établissements scolaires afin de faire des points de situation rapide en cas de danger ou de crise internationale soudaine susceptible de les mettre en danger.