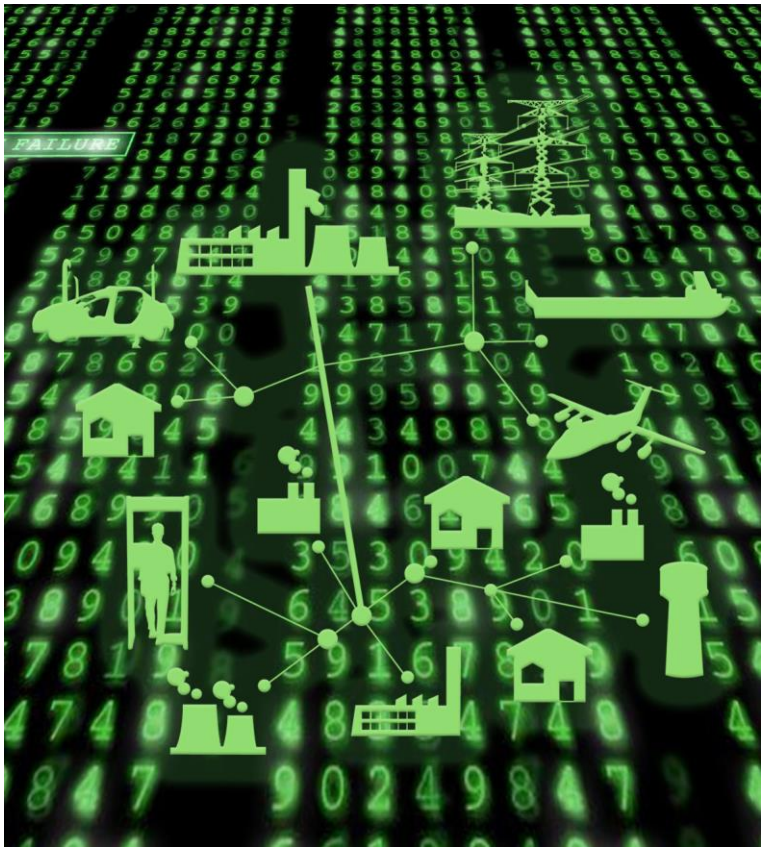
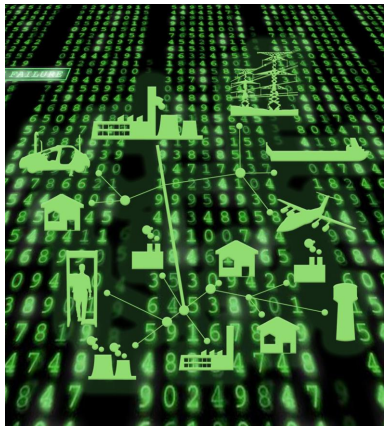
Réagir après l'attaque informatique



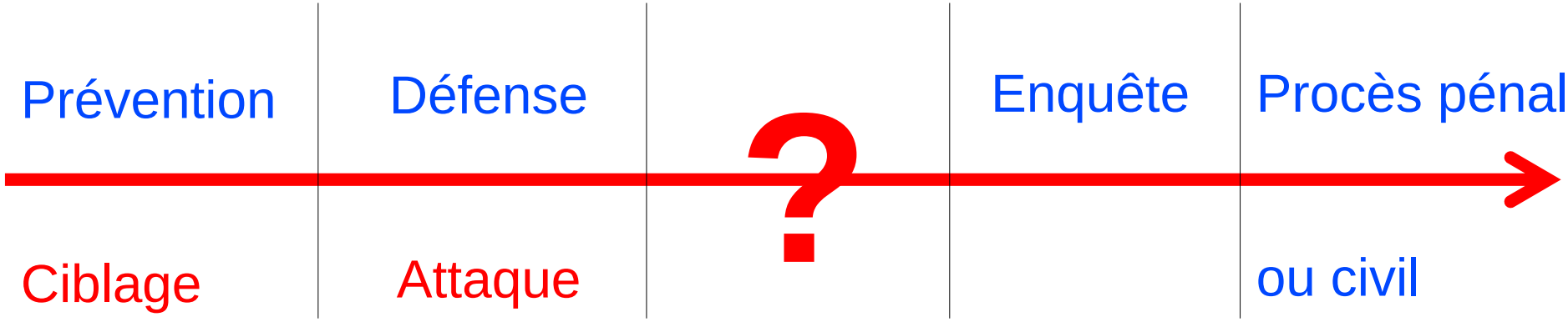
Philippe Davadie

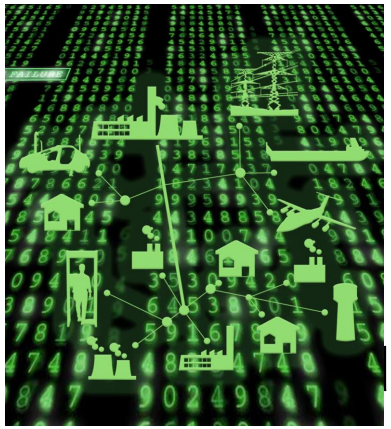
Gendarmerie Nationale

Groupe de travail de la Chaire Cyberdéfense & Cybersécurité



Axe des temps



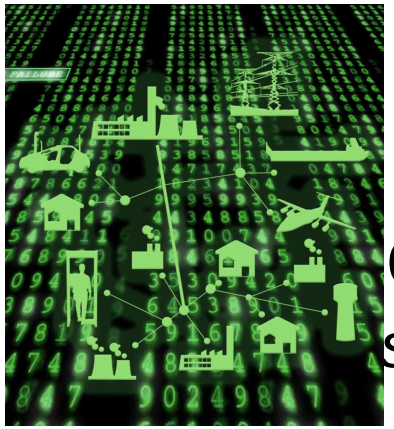


État des lieux

re abonde pour les mesures à prendre avant l'attaque et l'enquête judiciaire, elle est plus discrète entre ces deux événements.

Pourtant, l'enquête judiciaire fait suite à une plainte qui doit être initiée.

Il est donc indispensable que l'entreprise réagisse à toute attaque conformément à ses intérêts.



Avoir les idées claires

er panne/négligence/attaque *parmi le bruit*

s attaques.

Personnel sensibilisé et formé ?

Intention malveillante / Bring Your Own Disease / Audit logiciel.

Dispositif d'urgence ou de redémarrage

Recherche des causes de l'incident.

Colmater les brèches, tout en sauvegardant les preuves.

Recherche du mode opératoire.

Pas de légitime défense

Atteinte injustifiée, dans le même temps, strictement nécessaire, proportionné à la gravité de l'infraction (122-5 CP).

Danger actuel ou imminent, acte nécessaire à la sauvegarde de

Les mesures adéquates

r le mode opératoire.

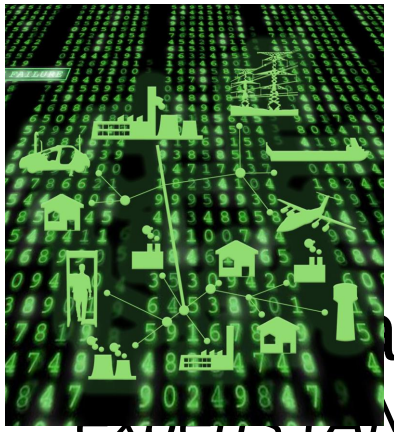
Analyser les causes. *Retex à mener (bureau de la confiance)*

En tirer les conséquences : *organisation, procédures.*

Diffuser l'information :

En interne (failles utilisées, mode opératoire, conséquences pour l'entreprise, nouvelles mesures à prendre) ;

En externe



Passer le relais

avec les partenaires de l'entreprise :

experts (ANSSI, OZSSI), préfecture, CCI, enquêteurs.

L'entreprise ne peut obtenir réparation seule.

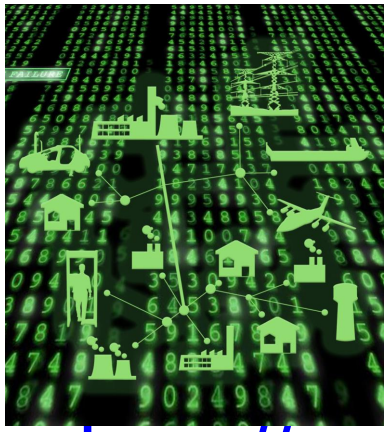
Réparations possible via :

l'assurance (impartialité des experts, principe d'inattribution) ;

la voie judiciaire :

civile (obtenir réparation d'un préjudice) ;

pénale (infraction punissable, tentative,



Documents utiles

http://www.informatiques-orphelines.fr

Questions à se poser avant la plainte *le pourcentage d'entreprises ayant déposé des plaintes suite à des incidents passe de 6% à 15% en 2014*

Aide mémoire du dépôt de plainte

Aide à la classification de l'information

Questions ?