

# SOUVERAINETE CYBER

## Rôles et problématiques

	AVANT ATTAQUE	PENDANT ATTAQUE	APRES ATTAQUE
<u>ACTIONS</u> -> (TEMPS LONG VS TEMPS COURT)	<u>EVALUATION</u> : - MENACES - VULNERABILITE - ETAT PREPARATION  <u>AUTONOMIE STRATEG</u> : - OUTIL INDUSTRIEL - R&D/INNOVATION - MAITRISE TECHNOLOG	<u>DETECTION</u> : - ANTICIPATION  <u>NATURE ATTAQUE</u> : - CIBLEE/MASSIVE - ESPIONNAGE - DESINFORMATION - DESTRUCTION - EXTORSION	<u>RESILIENCE</u> : - CONTINUITE DES OPERATIONS - MODE DEGRADE - BACKUP  <u>REPRISE</u>
<u>CIBLES</u> ↓ V	<u>PROTECTION</u> : - DISSUASION - FIREWALLS - CRYPTAGE - VEILLE  <u>PROTECTION</u> : - DISSUASION - FIREWALLS - CRYPTAGE - VEILLE  <u>ENVIRONNEMENT</u> : - ALLIANCES (EU/OTAN) - REGLEMENTATION INTERNATIONALE - STANDARDS - EMPIRES INDUS (GAFA)	<u>IDENTIFICATION DE L'AGRESSEUR</u> : - ETAT - GROUPE CRIMINEL - GROUPE POLITIQUE - INDIVIDU ISOLE	<u>RIPOSTE</u> - CYBER - JURIDIQUE - DIPLOMATIQUE - PHYSIQUE
<b>APPAREIL DE DEFENSE</b>			
<b>O.I.V. + INFRA STRUCTURES</b>			
<b>GOUVERNEMENT SERVICES PUBLICS</b>			
<b>ENTREPRISES</b>			
<b>PARTICULIERS</b>			