RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

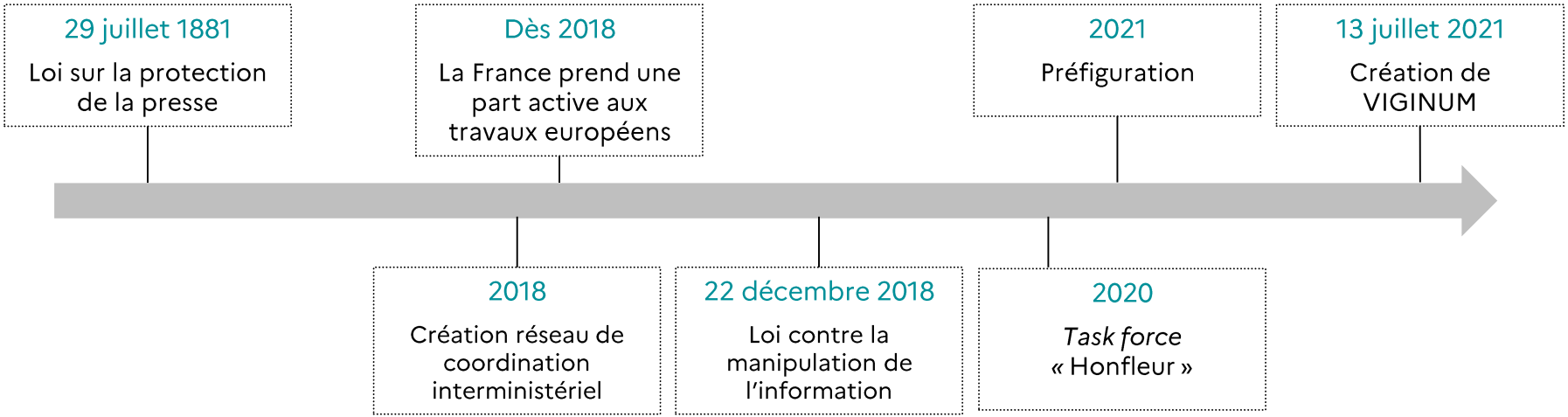
VIGINUM

RETOUR VERS LE CYBER

Quand la lutte contre les manipulations de l'information s'inspire des outils de la sécurité informatique

VIGINUM. L'historique du projet

Renforcer le dispositif national de lutte contre la manipulation de l'information pour détecter et analyser la menace



DÉFINITIONS

MANIPULATIONS DE L'INFORMATION

« Diffusion intentionnelle et massive de nouvelles fausses ou biaisées à des fins politiques hostiles »

J.B. JEANGÈNE VILMER, A. ESCORCIA, M. GUILLAUME, J. HERRERA, *Les manipulations de l'information*, rapport du CAPS, MEAE, IRSEM, ministère des Armées, Paris, août 2018, p. 12

INGÉRENCES NUMÉRIQUES ÉTRANGÈRES

- Implication d'un acteur étranger
- contenu manifestement inexact ou trompeur
- amplification inauthentique
- atteinte aux intérêts fondamentaux de la Nation

CIB

coordinated inauthentic behavior

2018

Meta

ABCDE

Actor

Behavior

Content

Degree/Distribution

Effect

Camille François (2019), Alexandre Alaphilippe (2020), James Pamment (2020)

The Cuckoo's Egg

1986

Mitre ATT&CK

2013

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drag-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys		Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media					Standard Cryptographic Protocol
	Scheduled Task	Hooking		File System Logical Offsets	Securityd Memory					Standard Non-
	Scripting			Gatekeeper Bypass	Two-Factor Authentication Interception					
	Service Execution									
	Signed Binary Proxy									

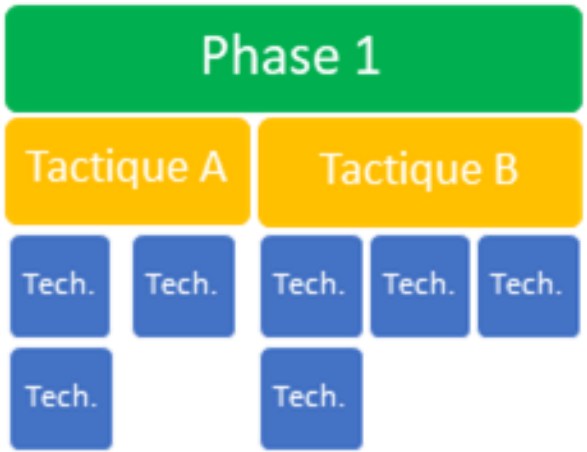
T1155

Misinfosec

Misinfosec working group
2018

Sara-Jayne Terp, Christopher R. Walker, John Gray, Pablo Breueur

DISARM


Phase 1
Tactique A
Tactique B
Tech.
Tech.
Tech.
Tech.
Tech.
Tech.
Tech.

DISARM Red Framework - incident creator TTPs

PLAN			PREPARE						EXECUTE						ASSESS
TA01: Plan Strategy	TA02: Plan Objectives	TA13: Target Audience Analysis	TA14: Develop Narratives	TA06: Develop Content	TA15: Establish Social Assets	TA16: Establish Legitimacy	TA05: Microtarget	TA07: Select Channels and Affordances	TA08: Conduct Pump Priming	TA09: Deliver Content	TA17: Maximize Exposure	TA18: Drive Online Harms	TA10: Drive Offline Activity	TA11: Persist in the Information Environment	TA12: Assess Effectiveness
T0073: Determine Target Audiences	T0002: Facilitate State Propaganda	T0072: Segment Audiences	T0003: Leverage Existing Narratives	T0015: Create hashtags and search artifacts	T0007: Create Inauthentic Social Media Pages and Groups	T0009: Create fake experts	T0016: Create Clickbait	T0029: Online polls	T0020: Trial content	T0114: Deliver Ads	T0049: Flooding the Information Space	T0047: Censor social media as a political force	T0017: Conduct fundraising	T0059: Play the long game	T0132: Measure Performance
T0074: Determine Strategic Ends	T0066: Degrade Adversary	T0072.001: Geographic Segmentation	T0004: Develop Competing Narratives	T0019: Generate information pollution	T0010: Cultivate ignorant agents	T0009.001: Utilize Academic/Pseudoscientific Justifications	T0018: Purchase Targeted Advertisements	T0043: Chat apps	T0039 : Bait legitimate influencers	T0114.001: Social media	T0049.001: Trolls amplify and manipulate	T0048: Harass	T0017.001: Conduct Crowdfunding Campaigns	T0060: Continue to Amplify	T0132.001: People Focused
	T0075: Dismiss	T0072.002: Demographic Segmentation	T0022: Leverage Conspiracy Theory Narratives	T0019.001: Create fake research	T0013: Create inauthentic websites	T0011: Compromise legitimate accounts	T0101: Create Localized Content	T0043.001: Use Encrypted Chat Apps	T0042: Seed Kernel of truth	T0114.002: Traditional Media	T0049.002: Hijack existing hashtag	T0048.001: Boycott/"Cancel" Opponents	T0057: Organize Events	T0128: Conceal People	T0132.002: Content Focused
	T0075.001: Discredit Credible Sources	T0072.003: Economic Segmentation	T0022.001: Amplify Existing Conspiracy Theory Narratives	T0019.002: Hijack Hashtags	T0014: Prepare fundraising campaigns	T0097: Create personas	T0102: Leverage Echo Chambers/Filter Bubbles	T0043.002: Use Unencrypted Chats Apps	T0044: Seed distortions	T0115: Post Content	T0049.003: Bots Amplify via Automated Forwarding and Reposting	T0048.002: Harass People Based on Identities	T0057.001: Pay for Physical Action	T0128.001: Use Pseudonyms	T0132.003: View Focused
	T0076: Distort	T0072.004: Psychographic Segmentation	T0022.002: Develop Original Conspiracy Theory Narratives	T0023: Distort facts	T0014.001: Raise funds from malign actors	T0097.001: Backstop personas	T0102.001: Use existing Echo Chambers/Filter Bubbles	T0103: Livestream	T0045: Use fake experts	T0115.001: Share Memes	T0049.004: Utilize Spamoflauge	T0048.003: Threaten to Dox	T0057.002: Conduct Symbolic Action	T0128.002: Conceal Network Identity	T0133: Measure Effectiveness
			T0040:		T0014.002: Raise	T0098:	T0102.002:		T0046:	T0115.002: Post Violative				T0128.003: Distance	

DISARM Red Framework - incident creator TTPs

PLAN			PREPARE						EXECUTE						ASSESS
TA01: Plan Strategy	TA02: Plan Objectives	TA13: Target Audience Analysis	TA14: Develop Narratives	TA06: Develop Content	TA15: Establish Social Assets	TA16: Establish Legitimacy	TA05: Microtarget	TA07: Select Channels and Affordances	TA08: Conduct Pump Priming	TA09: Deliver Content	TA17: Maximize Exposure	TA18: Drive Online Harms	TA10: Drive Offline Activity	TA11: Persist in the Information Environment	TA12: Assess Effectiveness
T0073: Determine Target Audiences	T0002: Facilitate State Propaganda	T0072: Segment Audiences	T0003: Leverage Existing Narratives	T0015: Create hashtags and search artifacts	T0007: Create Inauthentic Social Media Pages and Groups	T0009: Create fake experts	T0016: Create Clickbait	T0029: Online polls	T0020: Trial content	T0114: Deliver Ads	T0049: Flooding the Information Space	T0047: Censor social media as a political force	T0017: Conduct fundraising	T0059: Play the long game	T0132: Measure Performance
T0074: Determine Strategic Ends	T0075: Degrade Adversary	T0072.001: Geographic Segmentation	T0004: Develop Competing Narratives	T0019: Generate information pollution	T0010: Cultivate ignorant agents	T0009.001: Utilize Academic/Pseudoscientific Justifications	T0018: Purchase Targeted Advertisements	T0043: Chat apps	T0039 : Bait legitimate influencers	T0114.001: Social media	T0049.001: Trolls amplify and manipulate	T0048: Harass	T0017.001: Conduct Crowdfunding Campaigns	T0060: Continue to Amplify	T0132.001: People Focused
	T0075: Dismiss	T0072.002: Demographic Segmentation	T0022: Leverage Conspiracy Theory Narratives	T0019.001: Create fake research	T0013: Create inauthentic websites	T0011: Compromise legitimate accounts	T0101: Create Localized Content	T0043.001: Use Encrypted Chat Apps	T0042: Seed Kernel of truth	T0114.002: Traditional Media	T0049.002: Hijack existing hashtag	T0048.001: Boycott/"Cancel" Opponents	T0057: Organize Events	T0128: Conceal People	T0132.002: Content Focused
	T0075.001: Discredit Credible Sources	T0072.003: Economic Segmentation	T0022.001: Amplify Existing Conspiracy Theory Narratives	T0019.002: Hijack Hashtags	T0014: Prepare fundraising campaigns	T0097: Create personas	T0102: Leverage Echo Chambers/Filter Bubbles	T0043.002: Use Unencrypted Chats Apps	T0044: Seed distortions	T0115: Post Content	T0049.003: Bots Amplify via Automated Forwarding and Reposting	T0048.002: Harass People Based on Identities	T0057.001: Pay for Physical Action	T0128.001: Use Pseudonyms	T0132.003: View Focused
	T0076: Distort	T0072.004: Psychographic Segmentation	T0022.002: Develop Original Conspiracy Theory Narratives	T0023: Distort facts	T0014.001: Raise funds from malign actors	T0097.001: Backstop personas	T0102.001: Use existing Echo Chambers/Filter Bubbles	T0103: Livestream	T0045: Use fake experts	T0115.001: Share Memes	T0049.004: Utilize Spamoflauge	T0048.003: Threaten to Dox	T0057.002: Conduct Symbolic Action	T0128.002: Conceal Network Identity	T0133: Measure Effectiveness
			T0040:		T0014.002: Raise	T0098:	T0102.002:		T0046:	T0115.002: Post Violative				T0128.003: Distance	

PLAN

PREPARE

DISARM Red Framework - incident creator TTPs																
PLAN			PREPARE						EXECUTE							ASSESS
TA01: Plan Strategy	TA02: Plan Objectives	TA13: Target Audience Analysis	TA14: Develop Narratives	TA06: Develop Content	TA15: Establish Social Assets	TA16: Establish Legitimacy	TA05: Microtarget	TA07: Select Channels and Affordances	TA08: Conduct Pump Priming	TA09: Deliver Content	TA17: Maximize Exposure	TA18: Drive Online Harms	TA10: Drive Offline Activity	TA11: Persist in the Information Environment	TA12: Assess Effectiveness
T0073: Determine Target Audiences	T0002: Facilitate State Propaganda	T0072: Segment Audiences	T0003: Leverage Existing Narratives	T0015: Create hashtags and search artifacts	T0007: Create Inauthentic Social Media Pages and Groups	T0009: Create fake experts	T0016: Create Clickbait	T0029: Online polls	T0020: Trial content	T0114: Deliver Ads	T0049: Flooding the Information Space	T0047: Censor social media as a political force	T0017: Conduct fundraising	T0059: Play the long game	T0132: Measure Performance
T0074: Determine Strategic Ends	T0066: Degrade Adversary	T0072.001: Geographic Segmentation	T0004: Develop [illegible] Competin[illegible] Narrative[illegible]	[illegible] informa[illegible]on pollu[illegible]n	T0[illegible]: Cul[illegible] ign[illegible]nt ag[illegible]	T[illegible]09.00[illegible] Utiliz[illegible] Ac[illegible]emic/Pse[illegible]c Justifi[illegible]ons	T00[illegible] [illegible]e [illegible]arg[illegible]d A[illegible]ertise[illegible]nts	T0043: [illegible]hat apps	T0039 : Bait legitimate influencers	T0114.001: Social media	T0049.001: Trolls amplify and manipulate	T0048: Harass	T0017.001: Conduct Crowdfunding Campaigns	T0060: Continue to Amplify	T0132.001: People Focused
	T0075: Dismiss	T0072.002: Demographic Segmentation	T0022: Leverage Conspiracy Theory Narratives	T0019.001: Create fake research	T0013: Create inauthentic websites	T0011: Compromise legitimate accounts	T0101: Create Localized Content	T0043.001: Use Encrypted Chat Apps	T0042: Seed Kernel of truth	T0114.002: Traditional Media	T0049.002: Hijack existing hashtag	T0048.001: Boycott/"Cancel" Opponents	T0057: Organize Events	T0128: Conceal People	T0132.002: Content Focused
	T0075.001: Discredit Credible Sources	T0072.003: Economic Segmentation	T0022.001: Amplify Existing Conspiracy Theory Narratives	T0019.002: Hijack Hashtags	T0014: Prepare fundraising campaigns	T0097: Create personas	T0102: Leverage Echo Chambers/Filter Bubbles	T0043.002: Use Unencrypted Chats Apps	T0044: Seed distortions	T0115: Post Content	T0049.003: Bots Amplify via Automated Forwarding and Reposting	T0048.002: Harass People Based on Identities	T0057.001: Pay for Physical Action	T0128.001: Use Pseudonyms	T0132.003: View Focused
	T0076: Distort	T0072.004: Psychographic Segmentation	T0022.002: Develop Original Conspiracy Theory Narratives	T0023: Distort facts	T0014.001: Raise funds from malign actors	T0097.001: Backstop personas	T0102.001: Use existing Echo Chambers/Filter Bubbles	T0103: Livestream	T0045: Use fake experts	T0115.001: Share Memes	T0049.004: Utilize Spamoflauge	T0048.003: Threaten to Dox	T0057.002: Conduct Symbolic Action	T0128.002: Conceal Network Identity	T0133: Measure Effectiveness
		[illegible]	T0040: [illegible]	[illegible]	T0014.002: Raise [illegible]	T0098: [illegible]	T0102.002: [illegible]	[illegible]	T0046: [illegible]	T0115.002: Post Violative [illegible]	[illegible]		[illegible]	T0128.003: Distance [illegible]	[illegible]

DISARM Red Framework - incident creator TTPs

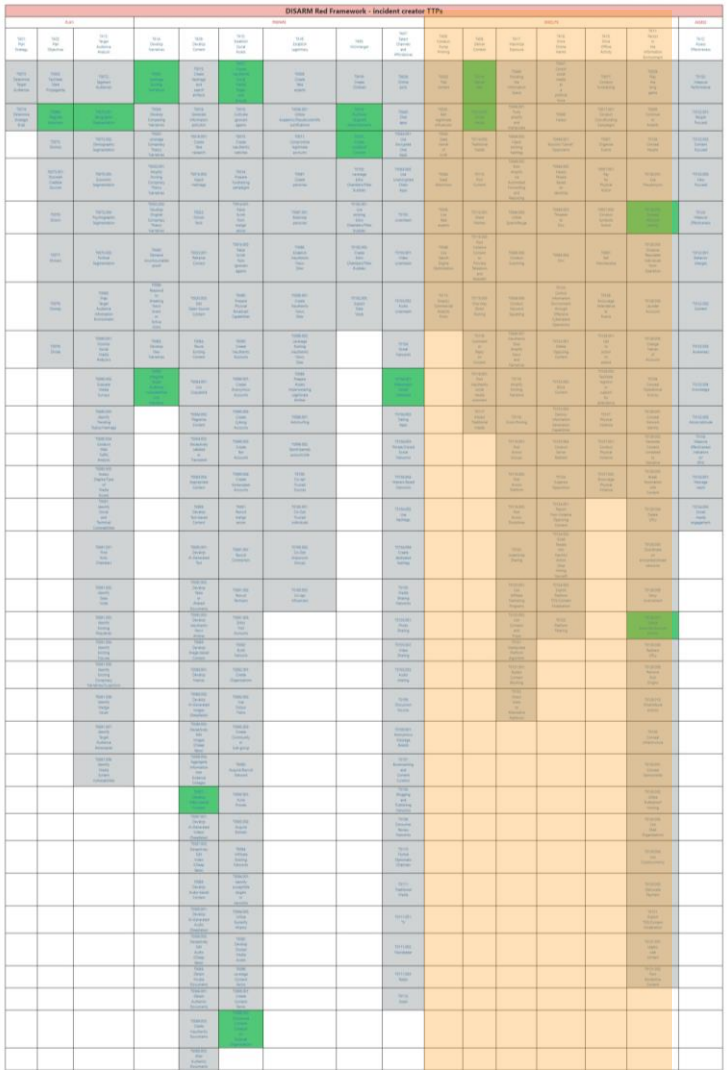
PLAN			PREPARE						EXECUTE						ASSESS
TA01: Plan Strategy	TA02: Plan Objectives	TA13: Target Audience Analysis	TA14: Develop Narratives	TA06: Develop Content	TA15: Establish Social Assets	TA16: Establish Legitimacy	TA05: Microtarget	TA07: Select Channels and Affordances	TA08: Conduct Pump Priming	TA09: Deliver Content	TA17: Maximize Exposure	TA18: Drive Online Harms	TA10: Drive Offline Activity	TA11: Persist in the Information Environment	TA12: Assess Effectiveness
T0073: Determine Target Audiences	T0002: Facilitate State Propaganda	T0072: Segment Audiences	T0003: Leverage Existing Narratives	T0015: Create hashtags and search artifacts	T0007: Create Inauthentic Social Media Pages and Groups	T0009: Create fake experts	T0016: Create Clickbait	T0029: Online polls	T0020: Trial content	T0114: Deliver Ads	T0049: Flooding the Information Space	T0047: Censor social media as a political force	T0017: Conduct fundraising	T0059: Play the long game	T0132: Measure Performance
T0074: Determine Strategic Ends	T0066: Degrade Adversary	T0072.001: Geographic Segmentation	T0004: Develop Competing Narratives	T0019: Generate information pollution	T0010: Cultivate ignorant agents	T0009.001: Utilize Academic/Pseudoscientific Justifications	T0018: Purchase Targeted Advertisements	T0043: Chat apps	T0039 : Bait legitimate influencers	T0114.001: Social media	T0049.001: Trolls amplify and manipulate	T0048: Harass	T0017.001: Conduct Crowdfunding Campaigns	T0060: Continue to Amplify	T0132.001: People Focused
	T0075: Dismiss	T0072.002: Demographic Segmentation	T0022: Leverage Conspiracy Theory Narratives	T0019.001: Create fake research	T0013: Create inauthentic websites	T0011: Compromise legitimate accounts	T0101: Create Localized Content	T0043.001: Use Encrypted Chat Apps	T0042: Kernel truth	[illegible]	T0049.002: [illegible]	[illegible] Opponents	[illegible]	[illegible]	T0132.002: Content Focused
	T0075.001: Discredit Credible Sources	T0072.003: Economic Segmentation	T0022.001: Amplify Existing Conspiracy Theory Narratives	T0019.002: Hijack Hashtags	T0014: Prepare fundraising campaigns	T0097: Create personas	T0102: Leverage Echo Chambers/Filter Bubbles	T0043.002: Use Unencrypted Chats Apps	T0044: Seed distortions	T0115: Post Content	[illegible] Bots Amplify via Automated Forwarding and Reposting	T0048.002: Harass People Based on Identities	T0057.001: Pay for Physical Action	T0128.001: Use Pseudonyms	T0132.003: View Focused
	T0076: Distort	T0072.004: Psychographic Segmentation	T0022.002: Develop Original Conspiracy Theory Narratives	T0023: Distort facts	T0014.001: Raise funds from malign actors	T0097.001: Backstop personas	T0102.001: Use existing Echo Chambers/Filter Bubbles	T0103: Livestream	T0045: Use fake experts	T0115.001: Share Memes	T0049.004: Utilize Spamoflauge	T0048.003: Threaten to Dox	T0057.002: Conduct Symbolic Action	T0128.002: Conceal Network Identity	T0133: Measure Effectiveness
			T0040:		T0014.002: Raise	T0098:	T0102.002:		T0046:	T0115.002: Post Violative				T0128.003: Distance	

EXECUTE

DISARM Red Framework - incident creator TTPs

PLAN			PREPARE						EXECUTE						ASSESS
TA01: Plan Strategy	TA02: Plan Objectives	TA13: Target Audience Analysis	TA14: Develop Narratives	TA06: Develop Content	TA15: Establish Social Assets	TA16: Establish Legitimacy	TA05: Microtarget	TA07: Select Channels and Affordances	TA08: Conduct Pump Priming	TA09: Deliver Content	TA17: Maximize Exposure	TA18: Drive Online Harms	TA10: Drive Offline Activity	TA11: Persist in the Information Environment	TA12: Assess Effectiveness
T0073: Determine Target Audiences	T0002: Facilitate State Propaganda	T0072: Segment Audiences	T0003: Leverage Existing Narratives	T0015: Create hashtags and search artifacts	T0007: Create Inauthentic Social Media Pages and Groups	T0009: Create fake experts	T0016: Create Clickbait	T0029: Online polls	T0020: Trial content	T0114: Deliver Ads	T0049: Flooding the Information Space	T0047: Censor social media as a political force	T0017: Conduct fundraising	T0059: Play the long game	T0132: Measure Performance
T0074: Determine Strategic Ends	T0066: Degrade Adversary	T0072.001: Geographic Segmentation	T0004: Develop Competing Narratives	T0019: Generate information pollution	T0010: Cultivate ignorant agents	T0009.001: Utilize Academic/Pseudoscientific Justifications	T0018: Purchase Targeted Advertisements	T0043: Chat apps	T0039 : Bait legitimate influencers	T0114.001: Social media	T0049.001: Trolls amplify and manipulate	T0048: Harass	T0017.001: Conduct Crowdfunding Campaigns	T0060: Continue to Amplify	T0132.001: People Focused
	T0075: Dismiss	T0072.002: Demographic Segmentation	T0022: Leverage Conspiracy Theory Narratives	T0019.001: Create fake research	T0013: Create inauthentic websites	T0011: Compromise legitimate accounts	T0101: Create Localized Content	T0043.001: Use Encrypted Chat Apps	T0042: Seed Kernel of truth	T0114.002: Traditional Media	T0049.002: Hijack existing hashtag	T0048.001: Boycott/"Cancel" Opponents	T0057: Organize Events	T0128: Conceal People	T0132.002: Content Focused
	T0075.001: Discredit Credible Sources	T0072.003: Economic Segmentation	T0022.001: Amplify Existing Conspiracy Theory Narratives	T0019.002: Hijack Hashtags	T0014: Prepare fundraising campaigns	T0097: Create personas	T0102: Leverage Echo Chambers/Filter Bubbles	T0043.002: Use Unencrypted Chats Apps	T0044: Seed distortions	T0115: Post Content	T0049.003: Bots Amplify via Automated Forwarding and Reposting	T0048.002: Harass People Based on Identities	T0057.001: Pay for Physical Action	T0128.001: Use Pseudonyms	T0132.003: View Focused
	T0076: Distort	T0072.004: Psychographic Segmentation	T0022.002: Develop Original Conspiracy Theory Narratives	T0023: Distort facts	T0014.001: Raise funds from malign actors	T0097.001: Backstop personas	T0102.001: Use existing Echo Chambers/Filter Bubbles	T0103: Livestream	T0045: Use fake experts	T0115.001: Share Memes	T0049.004: Utilize Spamoflauge				
			T0040:		T0014.002: Raise	T0098:	T0102.002:		T0046:	T0115.002: Post Violative				T0128.003: Distance	

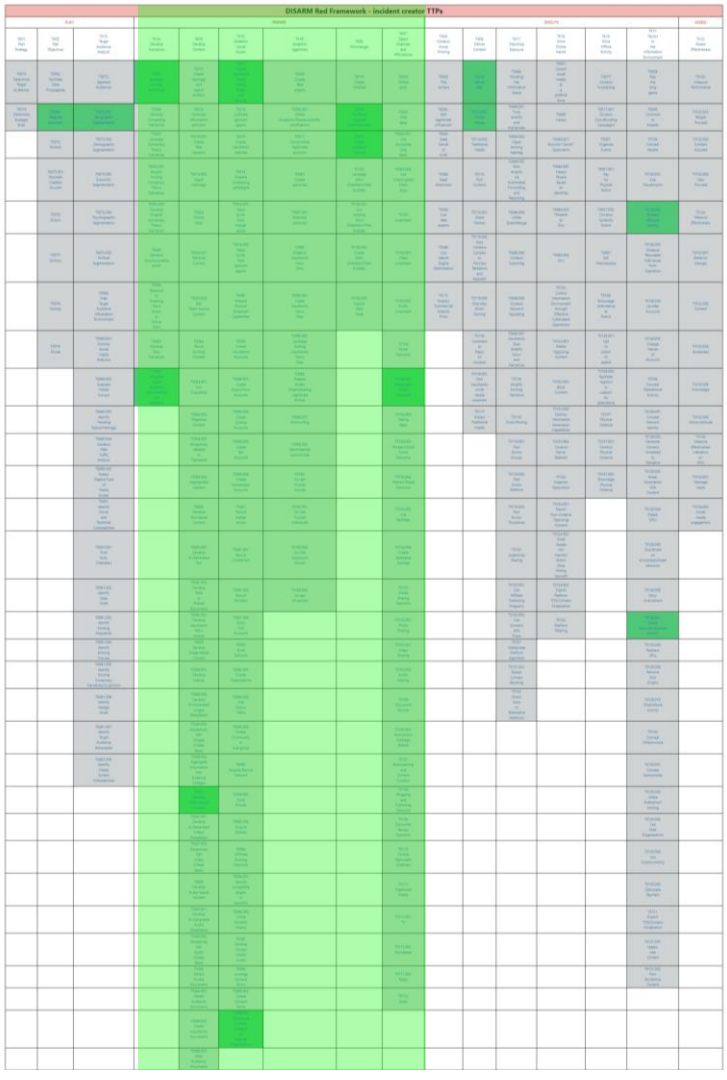
ASSESS



EXECUTE

T0114.001 : diffuser les publicités sur les réseaux sociaux

T0128.002 : dissimuler son activité en ligne



PREPARE

T0003 : exploiter des narratifs existants

T0083 : intégrer les vulnérabilités de l'audience ciblée dans les narratifs

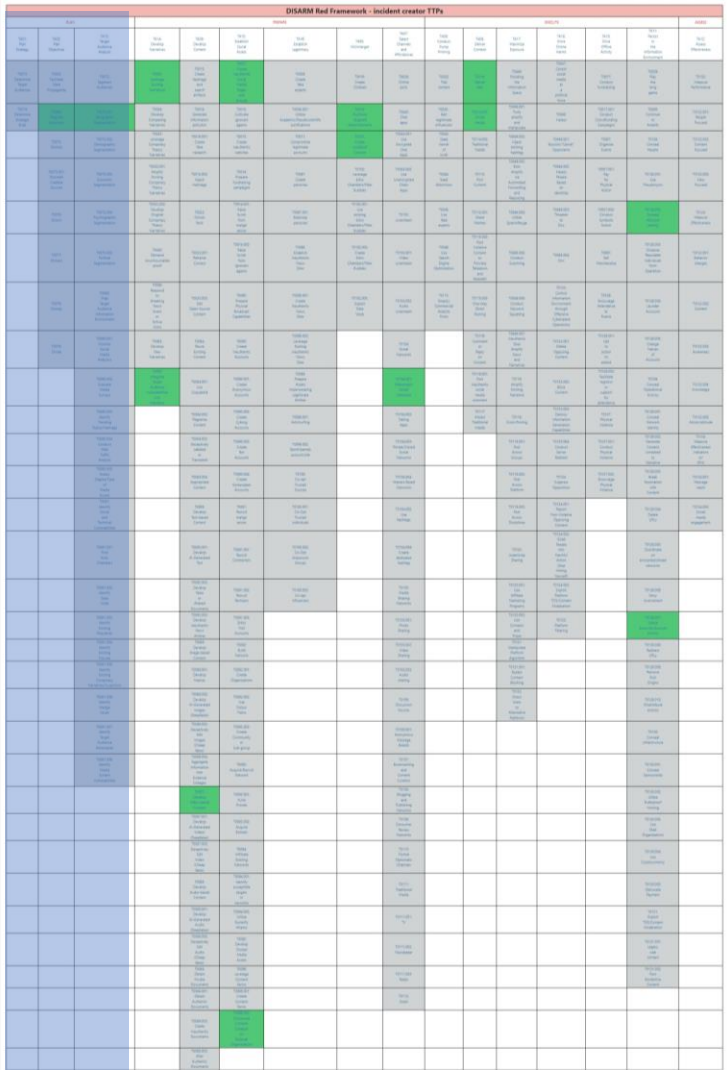
T0007 : créer des pages et des groupes inauthentiques de réseaux sociaux

T0096.002 : externaliser la création de contenu

T0018 : acquérir de la publicité ciblée

T0101 : créer du contenu localisé

T0104.001 : exploiter les réseaux sociaux généralistes



PLAN

T0066 : dégrader l'adversaire

T0072.001 : segmentation géographique de l'audience

PISTES DE TRAVAIL

https://www.sgdsn.gouv.fr/files/files/20221025-viginum-annee1.pdf.gouv.fr)