



Cryptage de données moderne avec approfondissement dans l'industrie militaire

Etudiante de 1re année d'Informatique
Anastasiia Kozlenko

Termes de cryptographie et de chiffrement à connaître



Cryptographie: la pratique de l'écriture et de la résolution de codes.

Clé: une chaîne secrète de caractères.

Cryptage: le processus mathématique de création et de partage d'un message codé.

Algorithme de chiffrement: ensemble d'algorithmes qui réalisent le chiffrement.

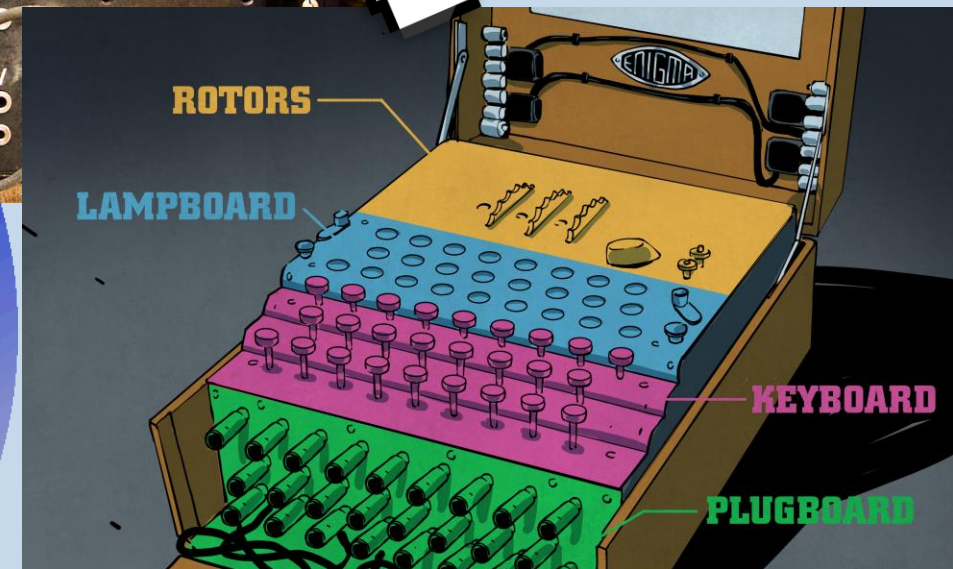
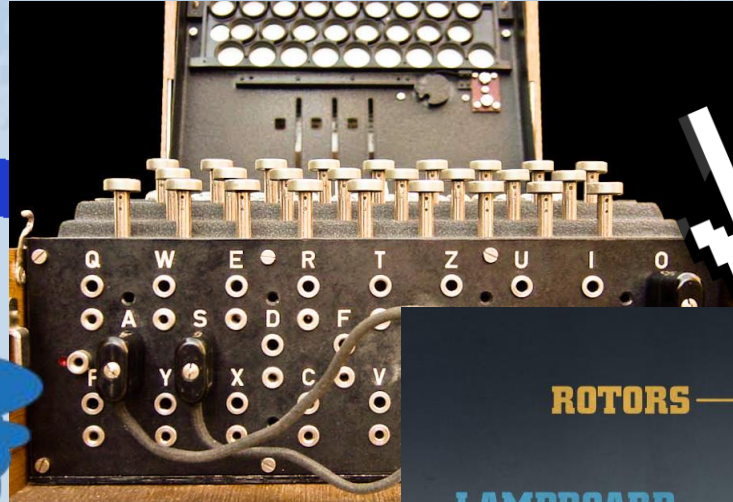
Ciphertext: la forme illisible d'un message codé.

Texte brut: le message décodé.

Le rôle de la cryptologie dans les deux conflits mondiaux

		Lettre en clair																											
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
Lettre de la clé		Lettres chiffrées (au croisement de la colonne <i>Lettre en clair</i> et de la ligne <i>Lettre de la clé</i>)																											
A		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		
B		B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A		
C		C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B		
D		D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C		
E		E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D		
F		F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E		
G		G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F		
H		H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G		
I		I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H		
J		J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I		
K		K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J		
L		L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K		
M		M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L		
N		N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M		
O		O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N		
P		P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O		
Q		Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P		
R		R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q		
S		S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R		
T		T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S		
U		U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T		
V		V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U		
W		W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V		
X		X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W		
Y		Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X		
Z		Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y		

Table de Vigenère

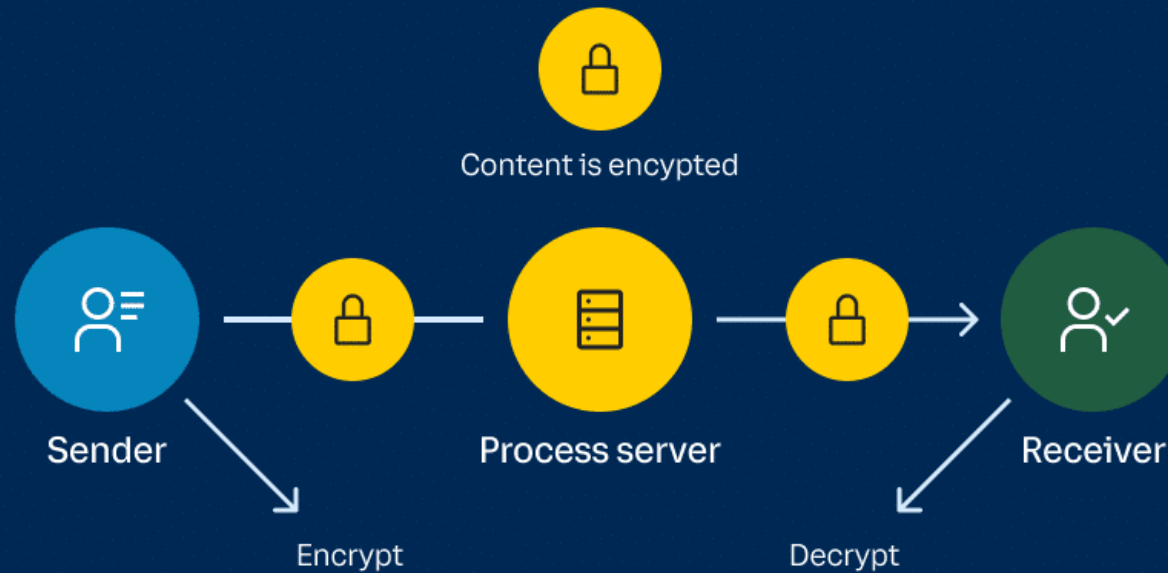


Machine Enigma



Le chiffrement de bout-en-bout

End-To-End Encryption

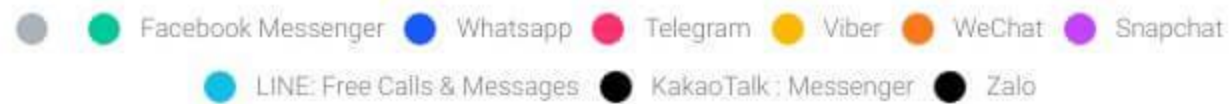


ires

rs actifs

Most Popular Messaging Apps by Country

(Android App Data: January -December 2022)



WhatsApp

WeChat

Facebook Messeng

Telegram





Snapchat 6

QQ mobile 574

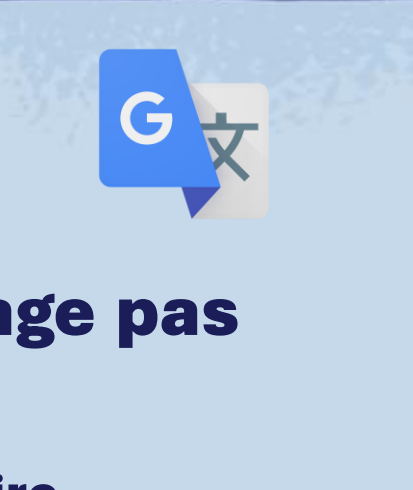
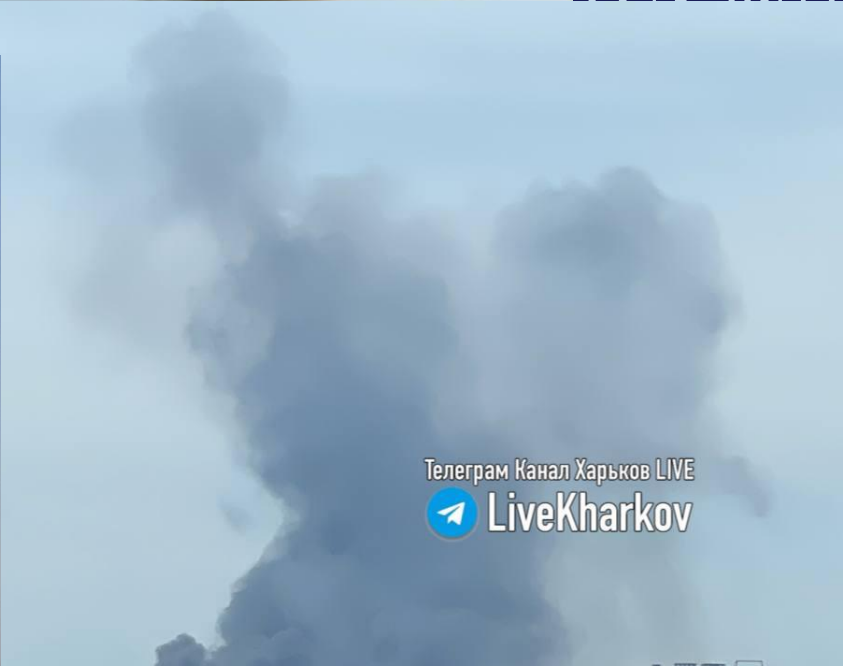
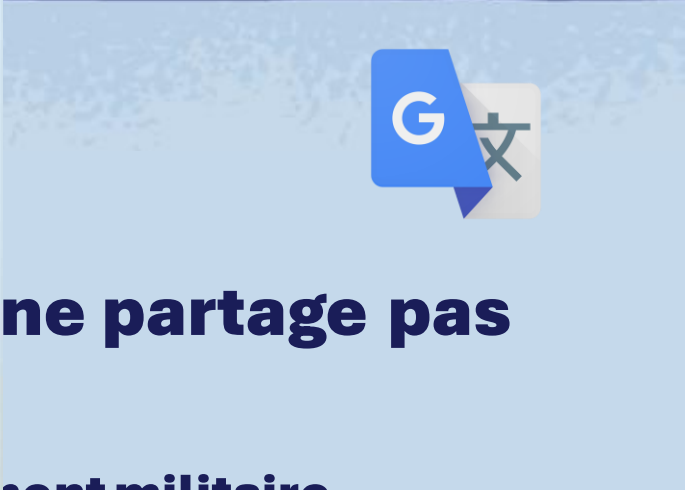
Viber 260

Discord 150

**Les plus populaires
≠
Les plus sécurisés**

Comparison										
Has refused to cooperate with intelligence agencies	✗	✗	✓	✗	✓	✓	✓	—	—	—
Provides transparency reports	✓	✓	✗	✓	✓	✓	✓	✓	✗	—
Abstains from collecting user data	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓
Default encryption	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓
Open source apps	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓
Open source servers	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗
Personal information is hashed	✗	✗	✗	✗	—	✓	—	✓	—	—
Encrypts metadata	✗	✗	✗	✗	—	✓	✓	—	—	—
Doesn't log timestamps and IP addresses	✗	✗	✗	✗	—	✓	✓	✓	—	—

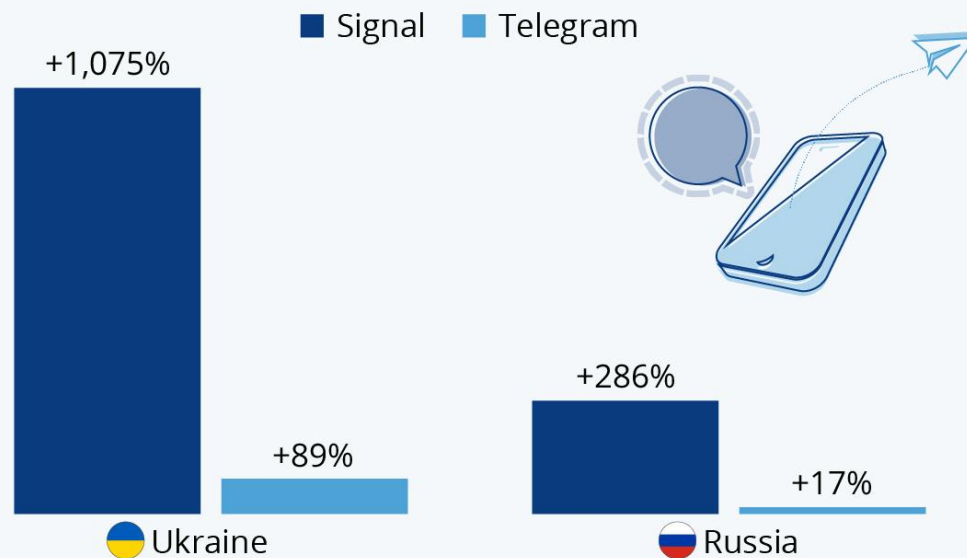
**Wickr
et Signal sont les
plus sécurisés**



Signal app

Growing Demand for Messaging Security in Ukraine and Russia

Pre- to post-invasion change in downloads of the encrypted apps Signal and Telegram in Ukraine and Russia*

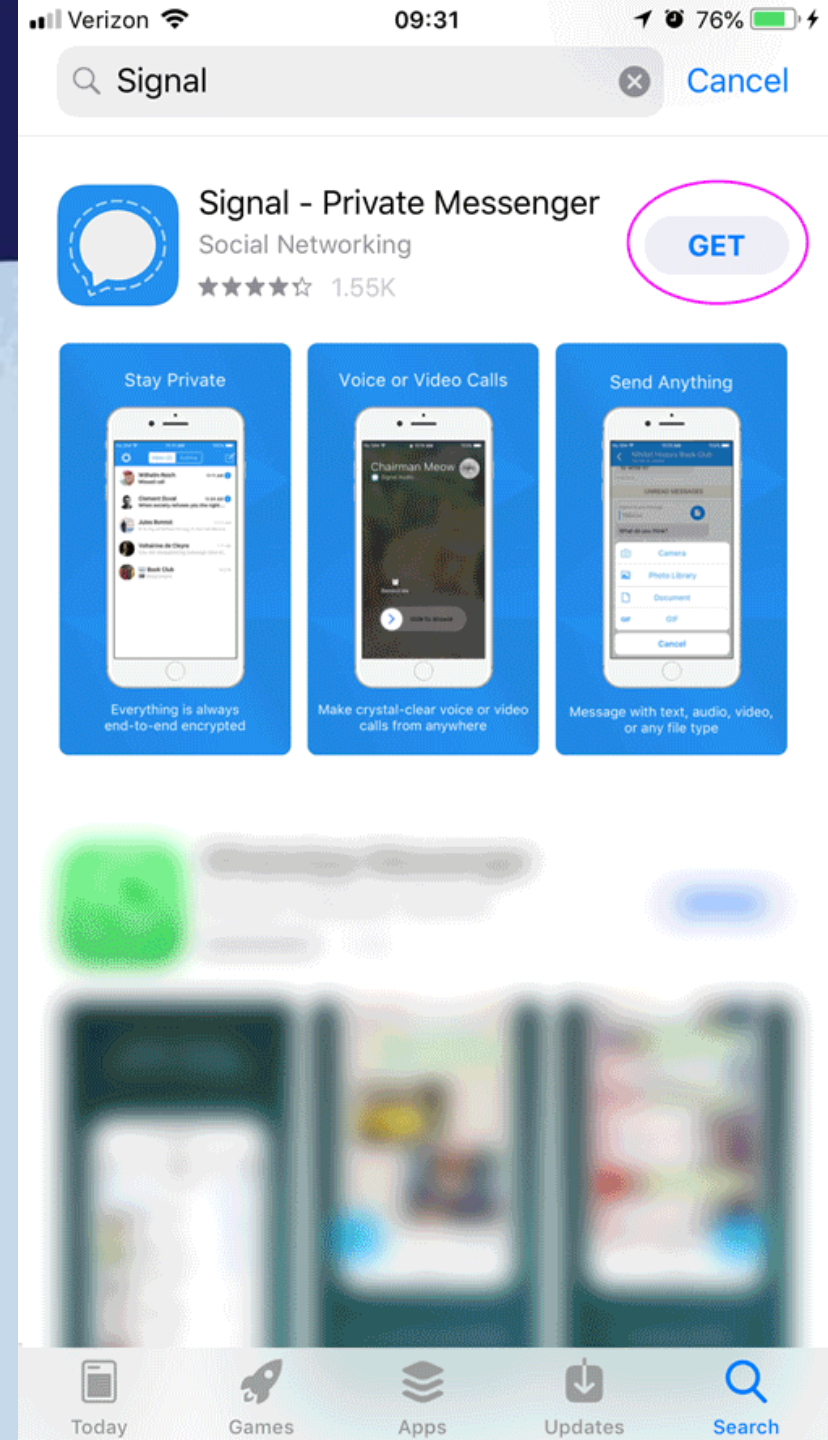


* Change from Jan 30 - Feb 23 to Feb 24 - Mar 20, 2022

Source: Sensor Tower



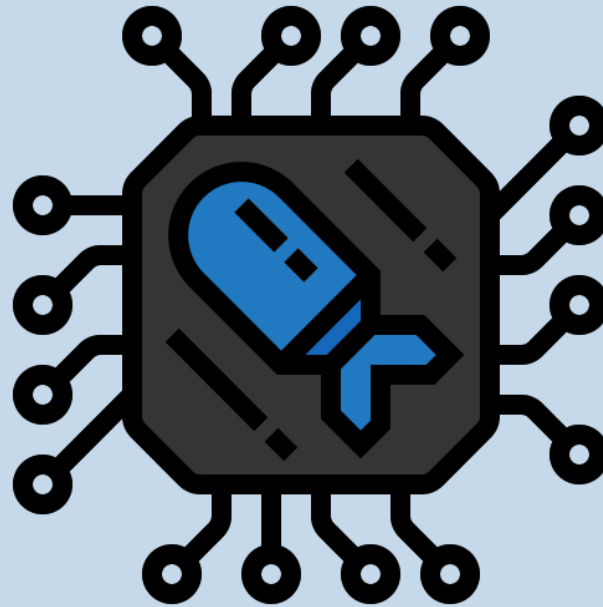
statista



Digitalisation de la guerre



Diia

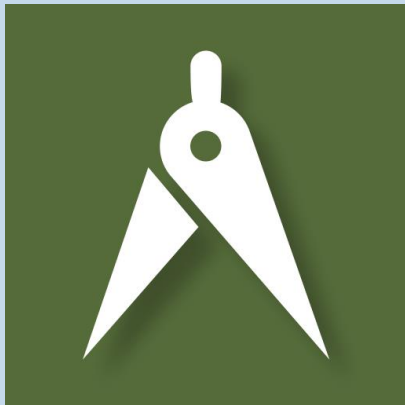
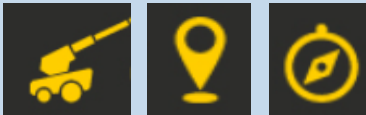


bot eEnemy

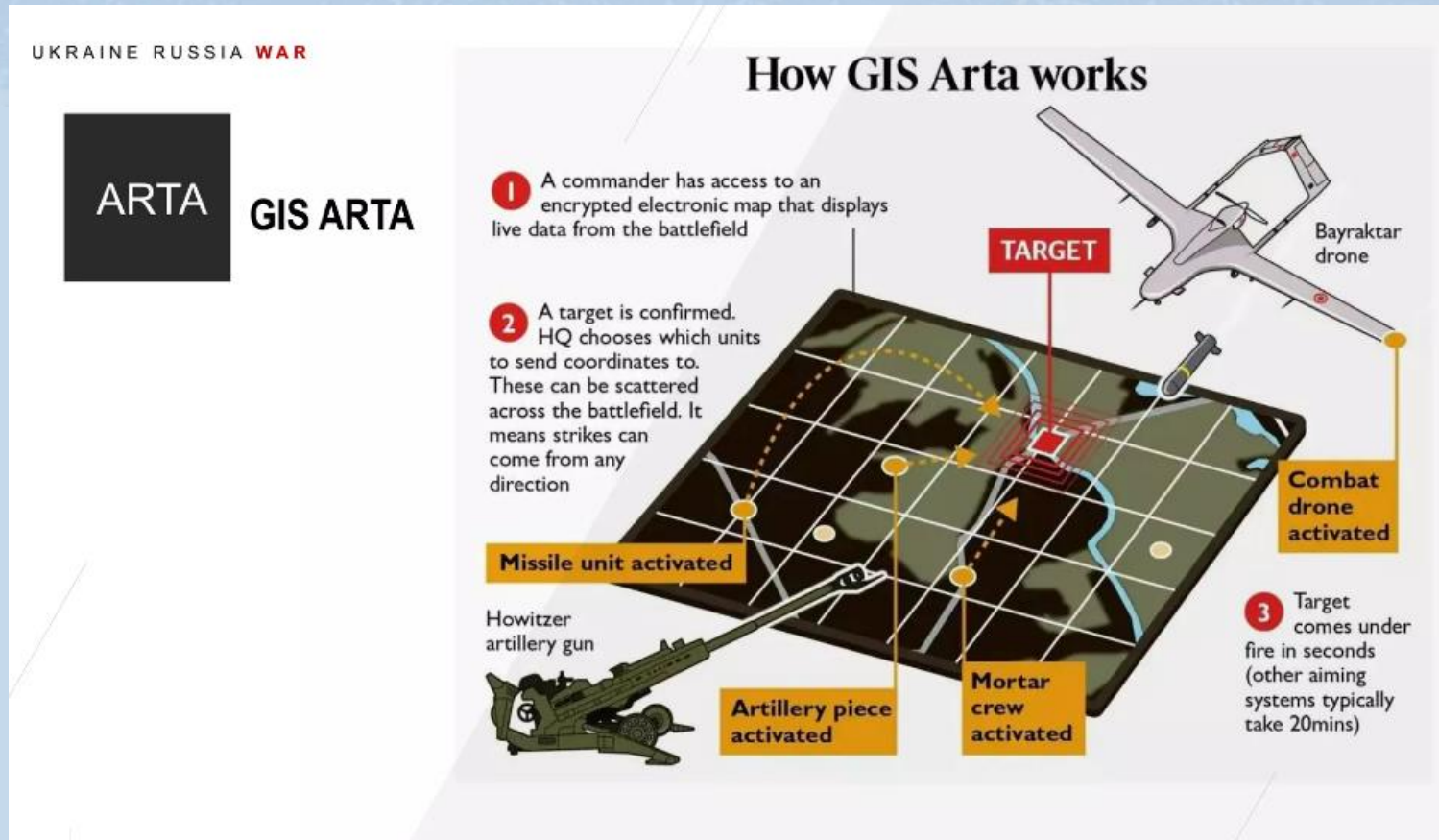
Digitalisation de la guerre



UkropSoft



TOPO

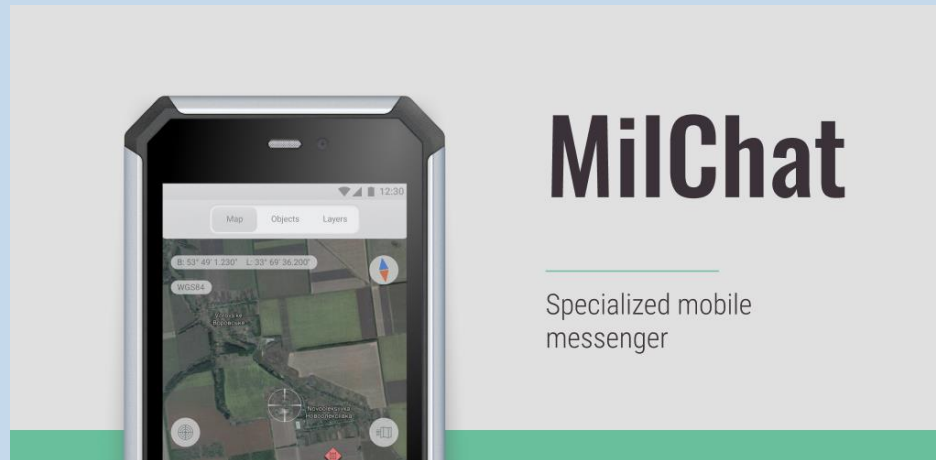


GIS ARTA

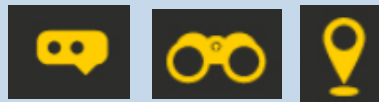
Digitalisation de la guerre



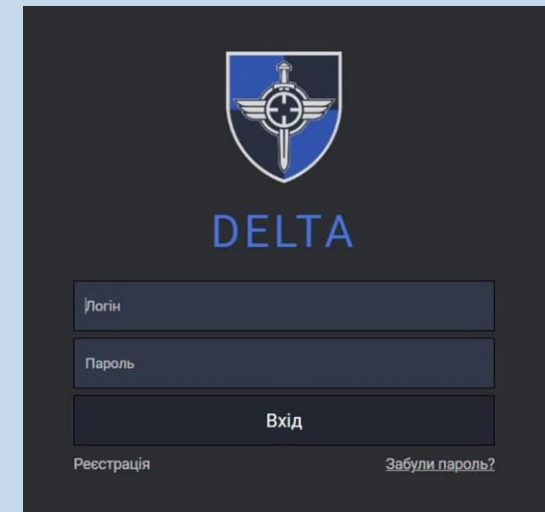
ComBat Vision



MilChat



ARMOR



Delta



Digitalisation de la guerre



Prostir (Espace)



Virage-tablette

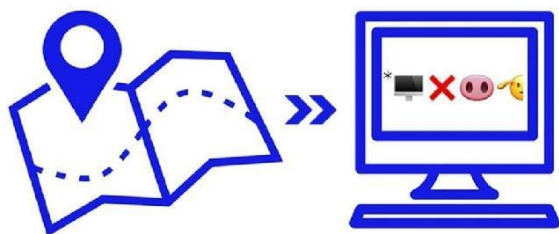


Véhicule de poste de commandement équipé "Bell"

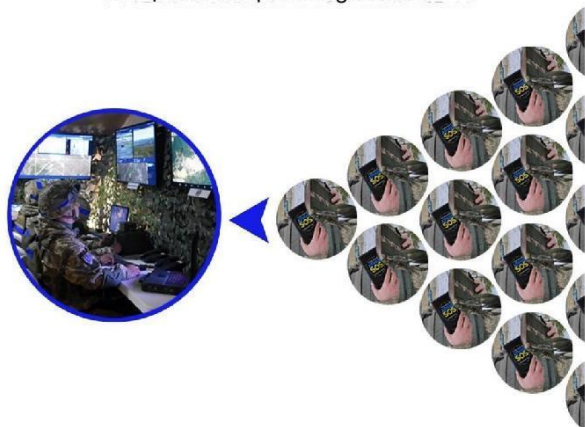
“Orties” l'App disruptive au service de la guerre

Complexe de quartier général
au lieu d'une carte avec
un crayon

Comment le complexe du quartier général du PC
"Kropyva", aide-t-il à détruire l'ennemi ?*



Désormais, l'armée utilise des tablettes
avec "Kropyva", à partir desquelles
les informations sont transmises au
complexe du quartier général !



Auparavant, toutes les positions étaient
marquées au crayon sur une carte papier.



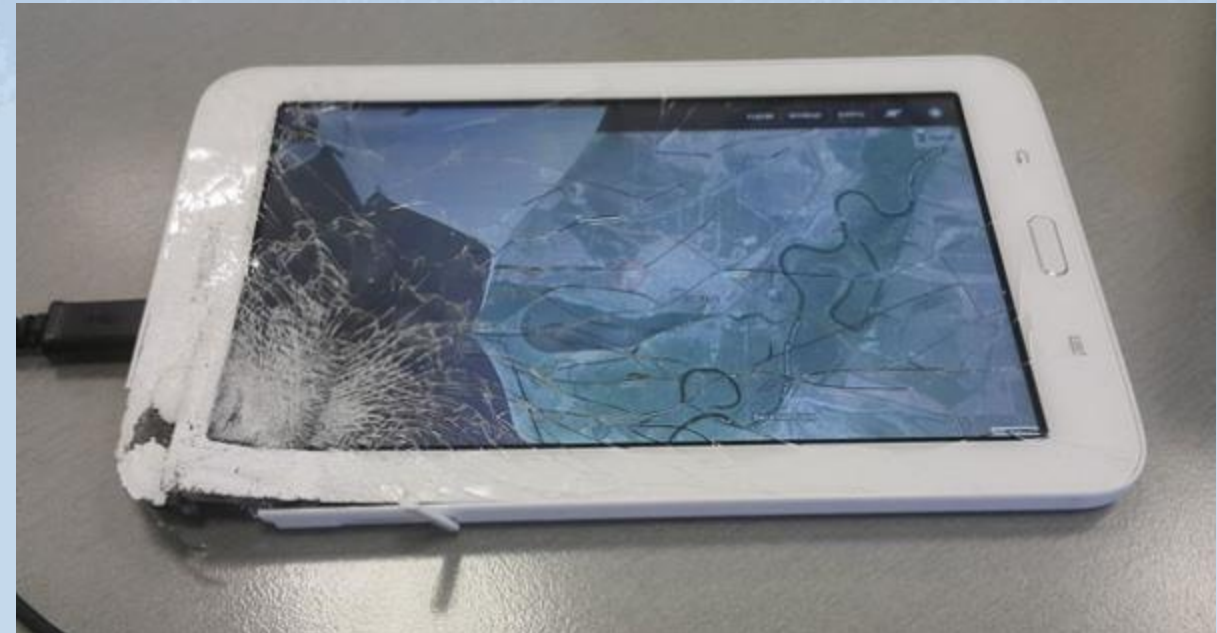
Le complexe du quartier général
permet au commandant de prendre des
décisions plus rapidement et de
gérer les unités



Automatic Tactical Management System



“Orties” l'App disruptive au service de la guerre



Conclusions



La cryptographie a maintenant une forme numérique

N'oubliez pas que vos données ne sont pas toujours cryptées



MERCI !

La façon de faire la guerre évolue, mais la protection des données est toujours au centre des préoccupations

