diploweb.com La revue géopolitique
ISSN : 2111-4307

La fiction permet-elle une immersion dans le combat cyber ? Entretien avec A. Namor et B. Boyer

dimanche 25 octobre 2026,par Anthony NAMOR, Bertrand BOYER, Pierre VERLUISE

Citer cet article / To cite this version :
Anthony NAMOR, Bertrand BOYER, Pierre VERLUISE, **La fiction permet-elle une immersion dans le combat cyber ? Entretien avec A. Namor et B. Boyer**, *Diploweb.com : la revue géopolitique, 25 octobre 2026.*

Hum... Vous semblez apprécier le DIPLOWEB.COM. Nous vous en remercions et vous invitons à participer à sa construction.

Le DIPLOWEB.COM est LE media géopolitique indépendant en accès gratuit, fondé en l'an 2000. Nous vous proposons de participer concrètement à cette réalisation francophone de qualité, lu dans 190 pays. Comment faire ? Nous vous invitons à verser une participation à votre convenance par PayPal via **la page suivante** . Vous pouvez aussi rédiger un chèque à l'ordre du DIPLOWEB.COM et l'adresser à Diploweb.com, Pierre Verluise, 1 avenue Lamartine, 94300, Vincennes, France. Ou bien encore faire un virement bancaire en demandant un RIB à l'adresse expertise.geopolitique@gmail.com.

Avec 5 000€ par mois, nous pouvons couvrir nos principaux frais de fonctionnement et dégager le temps nécessaire à nos principaux responsables pour qu'ils continuent à travailler sur le DIPLOWEB.COM.
Avec 8 000€ par mois, nous pouvons lancer de nouveaux projets (contenus, événements), voire l'optimisation de la maquette du site web du DIPLOWEB.COM.

Des auteurs qui ont une solide pratique du terrain cyber partagent leurs réflexions au moyen de nouvelles pour évoquer des menaces très réelles, présentes ou à venir. Une manière de mieux comprendre les actions et les acteurs sur le front cyber, en plein conflit, du niveau tactique au niveau stratégique. Anthony Namor et Bertrand Boyer publient le recueil « *Orages d'octets* », préface du général de corps d'armée Bruno Baratz, éditions de l'École de guerre, 2026. Ils répondent aux questions du *Diploweb.com*.

Pierre Verluise (P. V.) : Lorsqu'on lit ce recueil de nouvelles, on comprend que le cyber est un nouveau front de la guerre. C'est un peu « l'expérience du front du cyber » ? Serait-ce selon vous une bonne définition : un récit de *frontovniki* (pour reprendre un terme russe) du cyber ?

Anthony Namor (A. N.) : Dans une certaine mesure, c'est en effet l'angle que nous avons choisi et le sens du titre, « Orages d'octets », qui fait écho à l'œuvre d'Ernst Jünger « *Orages d'aciers* » (1920). Dans ce récit autobiographique, l'auteur témoignait des combats de tranchées qu'il avait vécus. Il décrivait une guerre née de l'ère industrielle, notamment marquée par un développement fulgurant de l'artillerie. Il ne s'agissait pas d'un nouveau front, mais d'un aspect de la guerre qui a pris une importance majeure, au point de transformer la tactique. De même, nous avons voulu décrire une guère née de l'ère informationnelle, dans laquelle le « cyber » (disons la lutte pour et par les moyens numériques de gagner un avantage sur l'ennemi), n'est pas un front en tant que tel, mais **un aspect des combats qui transforme la tactique**, c'est-à-dire les objectifs qu'on se fixe pour produire un effet sur l'ennemi, et la manière dont on les atteint. Tout comme la conquête des points hauts du terrain est devenue majeure (elle a toujours été un enjeu) lors de la Première Guerre mondiale pour positionner son artillerie ou ses points d'observation, la conquête des infrastructures matérielles comme logicielles est devenue essentielle pour maîtriser l'information qui permet de décider plus vite ou d'imposer son récit sur le champ de bataille.

L'idée était donc d'incarner cette réalité au travers de récits de fiction, pour sortir des écrits théoriques et sensibiliser le plus grand nombre.

Une autre inspiration de Jünger a peut-être été de trouver dans ces combats une forme d'aventure, de sport, sans bien sûr en nier le drame. Mais le parallèle s'arrête là : à l'inverse des *frontovniki*, nous n'avons pas vécu ce que nous écrivons. C'est un exercice de fiction, ancré dans le présent et ses développements, visant à réfléchir aux évolutions nécessaires à la victoire de demain.

> Dans cette guerre cyber, les civils sont en première ligne, souvent sans le savoir.

Bertrand Boyer (B. B.) : Le terme de *frontovniki* est séduisant, mais il contient un paradoxe que nous essayons justement d'effacer dans le livre. Dans l'imaginaire militaire, le combattant cyber est l'inverse du *frontovnik*, c'est un opérateur à distance, loin du danger physique. Ce que l'on souligne avec Anthony c'est que cette vision est aujourd'hui dépassée, ce que nous montre l'Ukraine et que nous projetons en 2042, **c'est au contraire le retour du combat au contact**. C'est l'arrivée massive de ces technologies au cœur même de la bataille. Cette dimension du conflit n'est plus une strate stratégique mais bien une composante essentielle de l'action du niveau tactique. Le cybercombattant revient à portée de drones, d'artillerie, parce que son émission électromagnétique le trahit et que son action doit être synchronisée avec la manœuvre. Au-delà, il y a également un nouveau front qui lui n'a ni arrière ni ligne de démarcation : celui des perceptions. Le smartphone du soldat, la page Facebook de sa compagne, le panneau d'affichage d'une ville assiégée deviennent

des terrains de lutte. Dans cette guerre, les civils sont en première ligne, souvent sans le savoir.

Orages d'octets, extrait de la couverture.
Cette illustration de Bertrand Boyer est un extrait de la couverture de Bertrand Boyer et Anthony Namor, « Orages d'octets », préface du général de corps d'armée Bruno Baratz, éditions de l'École de guerre, 2026. Droits réservés par Bertrand Boyer.
Bertrand Boyer

P. V. : Ce recueil de nouvelles, « Orages d'octets » (éd. de l'Ecole de guerre) décrit une attaque en 2042. Pourquoi 2042 particulièrement ? Cette réalité n'est-elle pas plus proche de nous ?

A. N. : Nous tenions à nous projeter dans un avenir assez proche pour entrer en résonnance avec ce que nous voyons des conflits contemporains. L'objectif est de réfléchir à cet avenir, autant que de vulgariser les enjeux de la guerre électronique, informatique et l'influence numérique d'aujourd'hui. Il est vrai que les choses évoluent si vite que nous avons parfois été dépassés par la réalité. Peu après la rédaction, tout début 2025, nous avons vu certains schémas tactiques et techniques imaginés dans nos nouvelles être réalisées en Ukraine ou en Iran.

Il nous fallait donc nous projeter « à horizon 2040 ». La date était trop proche de 2042 pour ne pas faire ce clin d'œil à la pop culture et aux fans de cyber (dans le guide du voyageur galactique, 42 est présenté comme la réponse ultime à toutes les questions. 42 a aussi de belles propriétés mathématiques et est largement employé comme un clin d'œil dans le domaine du numérique). Tant mieux si des néophytes le découvrent au détour d' « *Orages d'octets* » ! Le livre leur est tout à fait accessible, en particulier car chaque nouvelle est commentée et expliquée dans un texte succinct qui la suit.

B. B. : Il fallait trouver la bonne distance avec ce que nous avions vécu et ce que nous observons. Trop près, le texte aurait été lu comme une prévision, et chaque écart avec l'actualité l'aurait discrédité. Trop loin, on basculait dans la science-fiction, et le lecteur militaire aurait décroché, n'y trouvant pas matière à répondre aux problématiques de l'instant. Avec quinze ans d'écart, on dispose d'une liberté narrative tout en restant arrimé aux technologies existantes. **L'adoption de nouvelles technologies ne se fait pas en effaçant les autres mais par stratification, par ajout de couches supplémentaires**. Presque tout ce que nous décrivons existe déjà sous une forme ou une autre. Ce qui change, c'est la manière de l'employer et de le combiner. Sur ce point,

nous sommes plus proches de la démarche de la *Red Team* Défense que de Star Trek.

> Explorer des réponses différentes à des questions très actuelles.

P. V. : Vous utilisez des nouvelles pour évoquer des menaces très réelles. La fiction, c'est une manière d'imaginer des menaces à venir ou c'est simplement un moyen de nous faire prendre conscience des menaces présentes ?

A.N : Une grande partie des menaces présentées dans le livre est effectivement bien réelle aujourd'hui. Pour les expliquer et imaginer comment elles affecteront les combats de demain, la fiction offre plusieurs avantages. Elle permet d'abord de décrire des modes d'actions concrets sans dévoiler des opérations réelles – par nature sensibles. Elle oblige ensuite les auteurs à « tirer le fil » d'un fait nouveau. C'est l'exercice du « *what if* ? », que les officiers pratiquent déjà lorsqu'ils réfléchissent aux cas non conformes lors de la planification (que se passera-t-il si tel ou tel aspect du plan échoue ?). Par exemple, quelles sont les conséquences de l'électrification de nos véhicules ou de la robotisation du champ de bataille en termes de guerre électronique ? Enfin, la fiction offre un certain recul en permettant d'explorer des réponses différentes à des questions très actuelles : comment organiser nos états-majors pour trouver les meilleures solutions à des questions de plus en plus complexes ? Comment gérer la frontière entre vie privée et opérationnelle ? En tâchant de ne pas asséner de réponse péremptoire, mais en laissant le lecteur se faire son idée.

B. B : La fiction est une manière d'imaginer des menaces à venir et un moyen de faire prendre conscience des menaces présentes. J'ajouterais une dimension plus réflexive. **Les armées préparent toujours la guerre qu'elles sont capables d'imaginer**, et ce sont souvent des récits qui forgent ces représentations, bien avant la doctrine. Écrire de la fiction, c'est donc agir sur l'imaginaire de ceux qui préparent le combat de demain. Il y a aussi une forme de cohérence dans cette approche car, on ne peut pas parler sérieusement de lutte informationnelle sans prendre au sérieux le récit ! Nos adversaires l'ont compris depuis longtemps, eux qui mettent en récit leurs opérations, qui les bâtissent autour d'histoires plutôt que d'arguments. Enfin, la fiction permet de faire éprouver ce qu'un document de doctrine ne peut pas incarner : l'incertitude, la fatigue, le doute du décideur devant une information dont il ne sait pas si elle est vraie. Dans ce contexte **la fiction permet au lecteur une immersion que les essais théoriques interdisent**.

> Le retour de la haute intensité change la donne.

P. V. : Anthony Namor et Bertrand Boyer, ce recueil de nouvelles, « Orages d'octets » (éd. de l'Ecole de guerre) décrit les actions et les acteurs sur le front cyber, en plein conflit, du niveau tactique au niveau stratégique. En réalité n'y a-t-il pas un niveau plus concerné que l'autre par la menace ?

A. N. : Le cyber est une menace à tous les niveaux. Mais elle est aussi une formidable opportunité, en particulier au niveau tactique. C'est cette conviction que j'ai voulue partager au fil des nouvelles d'« Orages d'octets ». A mon sens, c'était un angle mort de la littérature traitant de cyberdéfense militaire. En effet, le « cyber » s'est historiquement construit « par le haut », au niveau stratégique. Au début des années 2010, les grandes puissances s'en sont saisi pour espionner, saboter, saper, dans une grande discrétion, nimbée de secret et de mystère, parfois propice aux fantasmes. Il

s'agissait alors de produire des effets stratégiques, dans la profondeur, sous le seuil de la violence assumée. Ces actions se déroulaient sur un temps long, nécessaire à la préparation comme à l'exploitation de l'attaque, nécessitait une expertise très poussée, pour un effet difficile à garantir et à maîtriser. Ces contraintes sont bien sûr incompatibles avec les besoins du niveau tactique, ce qui tend à discréditer l'appui cyber à ce niveau… car on raisonne pour le niveau tactique avec un logiciel stratégique, le seul que l'on connaisse à peu près.

Le retour de la haute intensité change la donne : la violence est assumée, une grande partie des combats a lieu en zone urbaine et périurbaine, la surface de contact numérique entre infrastructures civiles et militaires est de plus en plus importante, et la course à l'innovation des systèmes (logiciels, drones) laisse peu de place à la sécurité. Il y a donc une opportunité à saisir : exploiter des failles connues, utiliser et adapter des outils existants, assembler les briques « *open source* » d'une attaque « de l'électron au neurone », présente un coût très faible au regard des effets potentiels de telles actions. La véritable plus-value est tactico-technique : elle repose sur la maîtrise d'une chaîne d'attaque dont les composantes sont issues de la guerre électronique, de la lutte informatique offensive, de l'influence numérique. Cette cohérence nécessite des unités tactiques constituées, recrutées, formées et entraînées spécifiquement, et qui préfigurent peut-être des régiments ou bataillons cyber de demain.

B. B. : Ma démarche d'auteur reflète l'évolution décrite par Anthony. J'ai d'abord écrit « Cyberstratégie », puis « Cybertactique » deux ans plus tard, car il devenait évident que le sujet ne pouvait pas rester l'apanage des agences et des capitales. En 2014 nous faisions déjà face à des groupes terroristes qui utilisaient le cyber comme vecteur pour leurs opérations allant du recrutement en ligne à l'attaque informatique. Pourtant la vraie rupture me semble ailleurs et je la positionnerai plus dans l'écrasement des niveaux classiques (stratégique, opératif, tactique). **Dans l'espace informationnel, une action tactique peut produire instantanément un effet stratégique**. Une vidéo filmée par un soldat, une position trahie par une application de course à pied, un faux ordre qui circule : le « caporal stratégique » du général Krulak est devenu la règle depuis que l'accès à l'information s'est généralisé et partiellement dérégulé. Le danger le plus aigu tient moins à un niveau particulier qu'à cette porosité entre eux. Pour le commandement, la conséquence est lourde car il faut aujourd'hui accepter davantage de subsidiarité, tout en gardant la cohérence du récit d'ensemble. Les questions numériques se résument finalement souvent à ses deux notions de confiance et d'incertitude.

P. V. : Ce recueil de nouvelles, « Orages d'octets », met en scène plusieurs acteurs, civils ou militaires, dupés par des ruses cyber, qu'il s'agisse de transmettre inconsciemment un message d'attaque ou de commettre une erreur d'analyse stratégique. Le cyber est forcément lié à la duperie et à la ruse ?

A.N. : La duperie est une dimension importante du cyber, mais on peut attendre bien plus de cet appui. Dans les scénarios que l'on propose, il est vrai que les combinaisons guerre électronique ou informatique et opérations psychologiques sont très présentes. C'est peut-être lié à la complémentarité des auteurs, mais je pense surtout que ces combinaisons sont celles qui ont le plus de potentiel, qu'il s'agisse en effet de pirater des panneaux d'affichage pour diffuser des messages dans une ville assiégée, ou même d'authentifier des ordres en s'appuyant sur la *blockchain*. Mais l'appui cyber que l'on imagine offre aussi du renseignement, par l'exploitation de données ouvertes ou publicitaires recoupées par des sources plus classiques par exemple. De même il produit des effets, en aveuglant la coordination aérienne, en détournant des radars pour en faire des brouilleurs ou même en prenant le contrôle d'un véhicule autonome. Le point commun entre ces différentes actions est sans doute une forme de ruse, et d'opportunisme. En effet – et c'est un retournement notable de l'approche habituelle de la réflexion tactique – elles ne sont pas planifiées en partant d'effets à produire, mais résultent de la saisie d'opportunités concourant au plan.

> Le cyber ne réinvente pas la ruse, mais il change son économie.

B. B. : La ruse est une part essentielle de la guerre, et les exemples récents en Ukraine démontrent son importance pour redonner à la manœuvre les moyens de se développer. Le cyber ne réinvente pas la ruse, mais il change son économie. Avec l'intelligence artificielle générative, le faux est devenu presque gratuit : une voix, un visage ou un ordre se fabriquent en quelques minutes. L'armée française a déjà eu à faire face à ce type d'attaque lorsqu'au Sahel par exemple de faux ordres avait été diffusé sur les réseaux cherchant ainsi à créer une vague de réactions négative chez les populations. Plusieurs nouvelles explorent la conséquence de ce constat de **l'abaissement du coup d'entrée de la désinformation. Le défi n'est plus seulement de détecter le faux, mais d'être capable d'authentifier le vrai** [1]. L'adversaire peut gagner sans même nous tromper, simplement en créant le doute, en nous rendant soupçonneux de tout, y compris de nos propres informations. C'est ici que la guerre informationnelle trouve un domaine d'application encore à explorer puisqu'il vise directement les mécanismes cognitifs. Une armée qui ne croit plus ses capteurs ni ses ordres est paralysée plus certainement que par la destruction d'un relai télécom.

P. V. : Anthony Namor, Bertrand Boyer, qu'attendez-vous de ce livre, « *Orages d'octets* » (éd. de l'Ecole de guerre) ? Susciter des vocations ? Mieux comprendre les enjeux et les possibilités offertes par le cyber ? Quel serait le compliment le plus satisfaisant que vous pourriez entendre sur ce livre ?

A.N : J'espère que ce livre permettra d'appréhender le cyber à sa juste valeur dans les conflits modernes, dans ses opportunités comme ses limites. Ce faisant, je serais ravi qu'il suscite des vocations : élève en lycée militaire ou jeune lieutenant, j'aurais adoré lire ce livre. Un beau compliment pour moi serait : « j'ai appris et compris plein de choses sur le cyber et la guerre électronique, et je ne me suis pas ennuyé ! ».

B. B. : Pour ma part si un lecteur me disait « je n'avais jamais vu les choses ainsi » et si ce livre déplace un peu les représentations, alors je serai satisfait, il aura rempli sa mission. Enfin, s'il donne envie à quelques-uns de relire Jünger, ce ne sera pas mal non plus.

Copyright Octobre 2026-Namor-Boyer-Verluise/Diploweb.com

Plus

. Anthony Namor, Bertrand Boyer, « Orages d'octets ». Préface du général de corps d'armée Bruno Baratz. Editions de l'Ecole de guerre

4e de couverture

En septembre 2042, la Biélorussie décide d'envahir la Pologne, où une brigade de l'armée de Terre française s'entraîne aux côtés de son allié. La cyber guerre n'est alors plus un objet purement stratégique, fourbi en secret dans les couloirs d'agences nationales. Elle est conçue à portée de missiles, dans les centres opérations par les militaires qui s'affrontent, menée pied à pied par des civils volontaires, et jusque dans la boue du champ de bataille par les unités d'appui cyber électronique.
L'information est au cœur de la bataille : elle en façonne les buts comme les opportunités. En quoi

consiste ce combat invisible ? Pour dépasser la théorie, « Orages d'octets » décrit les arcanes du combat informationnel – de l'électron au neurone, de la conception des opérations à leur réalisation technique et tactique – au travers de neuf nouvelles de fiction commentées. Décideurs, analystes, techniciens et curieux y trouveront de quoi alimenter une indispensable réflexion sur la bataille de demain.

Saint-Cyrien, breveté de l'École de guerre, Bertrand Boyer est également diplômé de Telecom ParisTech et auditeur de l'IHEDN. Il a publié plusieurs ouvrages dans le domaine de la cyberdéfense et de la lutte informationnelle.
Saint-Cyrien, breveté de l'École de guerre, Anthony Namor a servi plus de dix ans en unités de guerre électronique et de cyberdéfense et été projeté plusieurs fois au Sahel.

P.-S.

Anthony Namor et Bertrand Boyer publient « *Orages d'octets* », préface du général de corps d'armée Bruno Baratz, éditions de l'École de guerre, 2026. Chacun s'exprime ici en son nom propre. Saint-Cyrien, breveté de l'École de guerre, Anthony Namor a servi plus de dix ans en unités de guerre électronique et de cyberdéfense et été projeté plusieurs fois au Sahel. Bertrand Boyer, saint-cyrien, breveté de l'Ecole de guerre, a notamment contribué au développement de la cyberdéfense et de la lutte informationnelle dans les armées en combinant expérience opérationnelle et approche conceptuelle.
Propos recueillis par Pierre Verluise docteur en Géopolitique, fondateur du *Diploweb.com*. Auteur, co-auteur ou directeur d'une trentaine d'ouvrages. Il est aussi le producteur de l'émission de radio Planisphère géopolitique et stratégique, disponible comme podcast sur les plateformes Spotify et Apple Podcast.

Notes

[1] NDLR. B. Boyer écrit : « Le défi n'est plus seulement de détecter le faux, mais d'être capable d'authentifier le vrai. » Nous pourrions ajouter : voire de garder le goût du vrai. En effet, un des effets des campagnes de désinformations des dernières années a été de dévaloriser, relativiser, voire annuler l'importance de ce qui est vrai. Les réseaux sociaux ont installé un comportement qui peut se résumer à : « Si ça me fait plaisir, je partage », même si on sait que ce n'est peut-être pas tout à fait exact.