C2 et Cyber.

Gilles Desclaux, Bernard Claverie

▶ **To cite this version:**

Gilles Desclaux, Bernard Claverie. C2 et Cyber.. Penser les Ailes Françaises, 2015, Réflexions sur le Cyber : Quels enjeux ?, 32, pp.61-68. hal-01672726

HAL Id: hal-01672726
https://hal.science/hal-01672726

Submitted on 24 Sep 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Copyright

ARMÉE DE L'AIR

Penser les Ailes françaises

La tribune de l'air et de l'espace

n°32
Juillet 2015

RÉFLEXIONS SUR LE CYBER : QUELS ENJEUX ?

MINISTÈRE DE LA DÉFENSE

Centre d'études stratégiques aérospatiales

Directeur de la publication :
GBA Patrice Sauvé, directeur du CESA

Rédacteur en chef :
Cdt Jean-Christophe Pitard-Bouet,
chef de la division études et rayonnement du CESA

Maquettage :
M. Emmanuel Batisse
M. Philippe Bucher
Clc Zita Martins Nunes
Av1 Antoine-David Da Silva Manteigas

Diffusion :
M. Pierre d'Andre
Clc Mathieu Cornu

Correspondance :
CESA
1 place Joffre – 75700 Paris SP 07 – BP 43
Tél. : 01 44 42 83 96 Fax : 01 44 42 80 10
www.cesa.air.defense.gouv.fr

Photogravure et impression :
Imprimerie EDIACA
Établissement d'impression, de diffusion et
d'archivage du commissariat des armées

Tirage : 2 500 exemplaires

C2 et Cyber

Général (2s) Gilles Desclaux et Monsieur Bernard Claverie
expert C2, Président de RACAM / Directeur de l'ENSC

Le C2, « Command and Control » ou « Commandement et Conduite », correspond à un ensemble de théories, de moyens et de méthodes de gestion de grands systèmes complexes, notamment dans le domaine des opérations militaires. C'est un modèle théorique qui s'articule autour des trois dimensions de la programmation de l'action coordonnée des forces et de la gestion des crises : la stratégie, la tactique et l'opérationnalité.

Le C2 est constitué d'une part de grands ensembles informatiques qui sont mobilisés dans la réception des informations,dans leur analyse, dans l'aide à la décision, dans la transmission des informations et des directives, dans la commande de l'action et son contrôle pour ajuster cette action en permanence aux objectifs recherchés. Ce premier volet, instrumental, est totalement empreint des dimensions du « cyber » dont il tire l'essence même de sa structure. Le C2 est d'autre part défini comme une organisation de gestion et un ensemble de procédures. Ce second volet permet de déterminer un ensemble hiérarchique et de délégations entre commandeurs et opérateurs pour organiser l'action des forces. Ces deux dimensions complémentaires, structurelle et fonctionnelle, constitue ce que l'on désigne aujourd'hui sous l'acronyme C4ISR-TAR. Il associe aux caractéristiques du commandement et de la conduite des opérations les dimensions et les outils de Contrôle, Communication, Computers, Intelligence, Surveillance, Reconnaissance, Target Acquisition et Reconnaissance spécifique (acquisition de cibles). Le C4ISR[1] est notamment le sigle utilisé par le Département de la Défense (DoD) américain et l'OTAN comme « *ensemble des moyens et des processus militaires organisés et structurés en vue de la conduite des opérations, de leur commandement et de leur contrôle* ».

1 Collectif (2015) : C4ISR & Networks. *Managing massive data (white paper)*. Washington (DC — USA) : Air Force Cyber Initiatives. - Joint Chiefs Of Staff Dod (2008), *Department Of Defense Dictionary Of Military And Associated Terms : Joint Publication* 1-02, Washington (DC, USA) : Government Printing Office (GPO), GPO Bookstore.

Un troisième volet est celui de l'étude théorique, qui s'affranchit des dimensions techniques et managériales, pour aborder une dimension générique du C2. Ce champ d'étude spécifique du « Command and Control » s'est ainsi constitué dans la conceptualisation des systèmes complexes[2], et c'est dans cette perspective que les auteurs examinent les influences du « cyber » sur la modélisation du C2 et sur les apports potentiels du C2 dans la gestion du « cyber ».

La machine C2

Le C2 peut être conçu comme une machine théorique et sa définition systémique s'inscrit dans la cybernétique[3]. Cette machine repose sur trois piliers : les trois côtés du triangle C2 (cf. figure 1) au sein duquel s'effectuent les grandes étapes du travail : la perception et l'analyse situationnelle, l'approche compréhensive de l'environnement et des moyens dont on dispose pour le modifier, la planification opérationnelle synthétisée par l'« *operational design* » et sa construction en lignes d'effort convergeant vers des centres de gravité (alliés, adversaires), et enfin le cycle de décision contingent des trois horizons temporels : *So what* ? *What if* ? *What next* ? qui comprend la synchronisation et la programmation des actions et l'évaluation constante des effets obtenus (*feedback*). La mise en œuvre des différentes boucles de contrôle et de *feed-back* mobilise de manière coordonnée les différents acteurs, moyens et soutiens au succès de l'opération. Ces côtés du triangle sont d'égale importance, et ils permettent l'entrée, la transformation puis la sortie d'information traitée par la machine C2 pour commander l'action de modification de l'environnement. Chacun de ces piliers est complémentaire et dépendant des autres et alimente la problématique « cyber ».

Le premier côté du triangle est celui des entrées et de la maîtrise de l'information. Il a pour but la « dominance informationnelle » et lui sont relatifs les différents renseignements, humain, d'open source et technologique : satellites, drones, radars et autres senseurs qui scrutent le spectre électromagnétique (*ISR dominance*). C'est par lui que transitent les informations entrantes (*inputs*) qui sont traitées, recombinées, conceptualisées, enrichies de manière physique et sémantique. C'est aussi le domaine de la gestion

2. Alberts, D.S., Hayes, R.E. (2006), *Understanding Command and Control*. Washington (DC, USA) : US Department of Defense, CCRP Publication Series.

3. Claverie, B., Desclaux, G. (2015), « La cybernétique : commande, contrôle et comportement dans la gestion des systèmes d'information et de communication ». *Hermes*, CNRS Éditions : 71, 72-79.

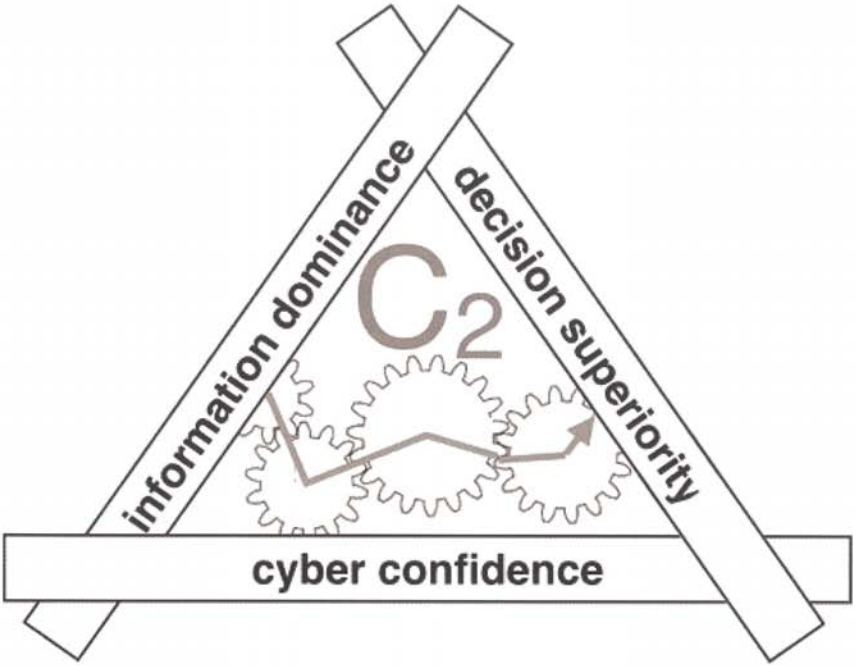


Figure 1 : la machine théorique du C2.

des connaissances, du *big data* et du *cloud computing*, de la corrélation et de la fusion des données, du ciblage intelligent (*video analytics, automated targeting workflow*)… Il permet de motiver une conscience de la situation partagée entre les différents étages du commandement et du contrôle, et d'évaluer les perspectives des réponses à l'action en fonction des moyens de recueil à programmer et à mettre en œuvre.

Le second côté est celui de la base du triangle. C'est sur lui que repose concrètement la machine avec l'ensemble des moyens matériels informatiques et des méthodes de calcul, de détection et d'imagerie. C'est sur lui que s'étaye la « *confiance informationnelle calculatoire* ». S'y rattachent les critères d'intégrité des réseaux, des calculateurs et des programmes, mais également le volet humain des relations, des interfaces et de l'intégration homme-système pour une forme de cyber résilience et de cyber agilité.

Le dernier côté est celui de la sortie de la machine C2. Il est orienté vers les effets désirés dans la constante de temps nécessaire et avec la précision temporelle souhaitée. C'est sur ce côté que s'appuient les différentes dimensions cognitives avec, notamment, l'unification et le partage des représentations, les processus de prise de décision collaborative en rapport avec les orientations du commandeur, les processus de gestion des opportunités et la programmation

critique et partagée de l'action par les différents vecteurs. Chacun de ceux-là, avion, drone, opérateur ou combattant, est lui-même soumis pour son action à une réplication de structure caractérisée par les 3 dimensions précédentes.

Cette machine C2 est inscrite dans une dynamique qui s'adapte aux demandes du pouvoir politique pour déterminer une flèche stratégique et pour produire des effets adaptés (cf. figure 2). Il est alors aisé de comprendre que dans un monde caractérisé par la convergence du « tout numérique » et par les nouveaux médias d'action de l'ennemi moderne, le « cyber » est à la fois un outil pour la théorisation du C2 et un domaine de contraintes qu'il doit prendre en compte. Sans reprendre les différentes menaces, les fragilités, les process de résilience et les moyens de correction, de protection ou d'efficacité mis en œuvre et largement développés dans le « cyber », l'évolution du domaine C2 est largement impactée par ces nouveaux paramètres. Le champ d'étude aborde aujourd'hui trois niveaux de complexité du système C2 : la complexité d'incertitude, la complexité dimensionnelle, la complexité computationnelle[4]. Chacun de ces niveaux est concerné par le « cyber ».

Les complexités « cyber » du C2

La complexité due à l'incertitude de l'information est, pour certains auteurs, le « grand défi » du C2[5]. Celui-ci est relatif à trois dimensions : l'incertitude technologique, l'incertitude de la situation et l'incertitude du facteur humain. C'est la problématique « cyber » qui permet de s'attacher à minimiser ces incertitudes et de tendre à ramener la situation à un état de relative efficience. Un premier domaine de préoccupation pour le C2 est relatif à différentes dimensions techniques, de MCO, de fusion et calcul, de limite technique... S'y ajoute la réduction pour une représentation imagée souvent immédiate et à destination d'opérateurs en situation opérationnelle complexe. La dimension « cyber » est ici celle de la réduction l'incertitude dans les deux dimensions, techniques et humaines. Si une autre voie d'incertitude est due aux activités humaines extérieures, volontaires ou

4. Cooper, C. (1994), « Complexity in C3I systems ». In D. Green et T. Bossomaier (Eds.) *Complex systems : from biology to computation*. Amsterdan (Pays Bas) : IOS Press, 223-231.

5. Levis, A. H., Athans, M. (1988), « The quest for a C3 theory : dreams and realities ». In S.E. Johnson et A.H. Levis (Eds.) *Science of Command and Control : coping with uncertainty*. Washington (DC, USA) : AFCEA International Press (Armed Forces Communications and Electronics Association), 4-9.

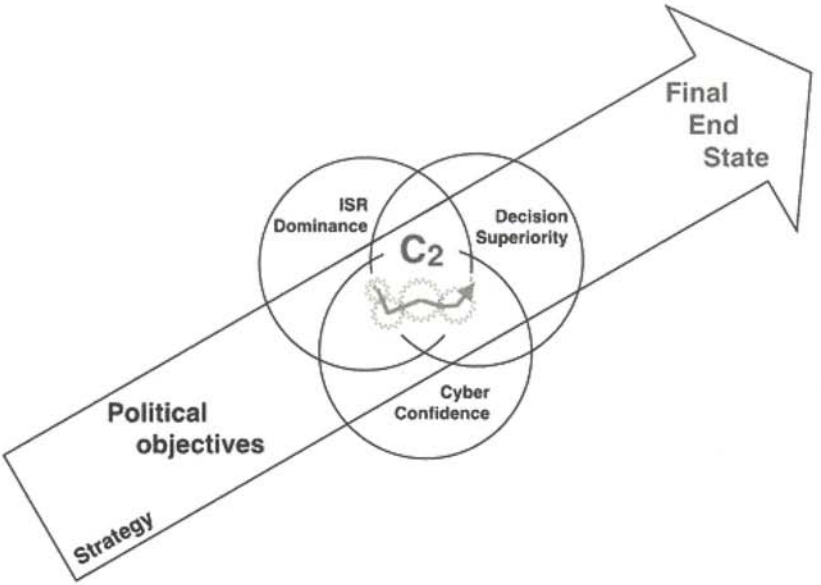


Figure 2 : le pouvoir transformateur de l'information par la machine C2.

non, la principale source est paradoxalement interne, relative aux propres faiblesses des acteurs du système. Le « facteur humain » est celui qui est le plus difficile à évaluer, comprendre, et à maîtriser. Il est cause de biais et d'erreurs qui créent cette incertitude de manière d'autant plus dangereuse qu'elle est souvent produite de bonne foi, susceptible d'être mal maîtrisée et passer inaperçue. Dans ce cadre, l'enjeu de l'ingénierie humaine est de traiter les causes de l'incertitude, en travaillant sur la robustesse des procédures, sur le partage représentationnel, sur la confiance relationnelle pour la maîtrise de l'erreur dans les systèmes complexes[6]. Ces domaines sont aujourd'hui peu étudiés dans le monde « cyber » et participent pour certains à quelques lieux de faiblesse significatifs du C2.

Un deuxième domaine d'influence « cyber » dans le C2 est relatif à la complexité dimensionnelle. Elle correspond au fait qu'un système de commande et de contrôle est structuré de manière cybernétique, en une hiérarchie de sous-systèmes en interaction mutuelle. Le nombre de cas à considérer augmente de manière exponentielle alors que chaque élément peut produire des quantités considérables d'informations dans un système fractal. Sa compréhension dépasse les capacités de compréhension et de représentation spontanée, les capacités de modélisation et surtout les moyens de leur calcul, engageant le C2 dans une véritable « malédiction de la dimensionnalité[5] ».

6. Strauch, B. (2007), *Investigagting Human Error : Incidents, Accidents, and Complex Systems*. Aldershot (UK) : Ashgate.

La complexité de calcul concerne les paramètres de rapidité, de fiabilité et de puissance de calcul. Ces dimensions classiques du monde « cyber » font entrer le C2 et son immense quantité de données dans celui du « *big data* ». Ceux qui en maîtrisent l'exploitation sont probablement les détenteurs du techno-pouvoir de demain. Son exploitation commence bien entendu par la maîtrise des capteurs mais également par le traitement des données ouvertes, de l'« open source », et de l'information « broadcast »[7] dans un monde dont la raison numérique est aujourd'hui soumise à la logique de l'exponentiel.

L'aide cognitique pour le C2

L'exploitation de l'information ouvre sur le domaine du « *data mining* » et celui de l'« intelligence artificielle ». Les techniques d'IA sont entrées depuis longtemps dans les différentes dimensions du C2[8]. L'IA et l'iconographie statistique constituent la base de la nécessaire réification des données. L'ensemble des informations est, à chaque étage de décision, le reflet plus ou moins fidèle de certaines caractéristiques physiques du milieu, de la nature d'événements qui s'y produisent, et de données artificielles surajoutées pour une forme d'« illusion du monde ». Il permet à chaque niveau d'avoir une certaine conscience du réel. Si les « *data* » sont censées en être des descriptions, elles sont transformées et interprétées, et ne parviennent au commandeur que de manière spéculaire.

Or une donnée interprétée est plus ou moins discutable, et la démarche de C2 va alors être d'en fournir un inventaire avec des algorithmes de réponse immédiate ou différée en fonction de critères de choix que supportent de nécessaires méta-systèmes d'intelligence artificielle. Elle termine avec sa synthèse par l'intelligence humaine, ainsi entraînée dans un exercice « cyber-cognitif » toujours plus difficile. Le C2 est donc un exercice hybride, inter et transdisciplinaire. Il associe aux dimensions techniques des plus grands programmes informatiques actuellement connus de ce côté de l'Atlantique pour traiter d'immenses quantités de données en perpétuelle évolution, les algorithmes de l'aide cognitive pour alimenter la gestion humaine d'opérations dont l'enjeu engage la sécurité de nos sociétés.

---

7. Alberts, D.S., Hayes, R.E. (2004), *Power to the Edge : Command, control, in the information age*. Information Age Transformation Series. Washington (DC, USA) : US Department of Defense CCRP Publication Series.

8. Taylor, E.C., Snell, D.J. (1988), « Artificial intelligence in command and control », *Signal*, 4, 25-29

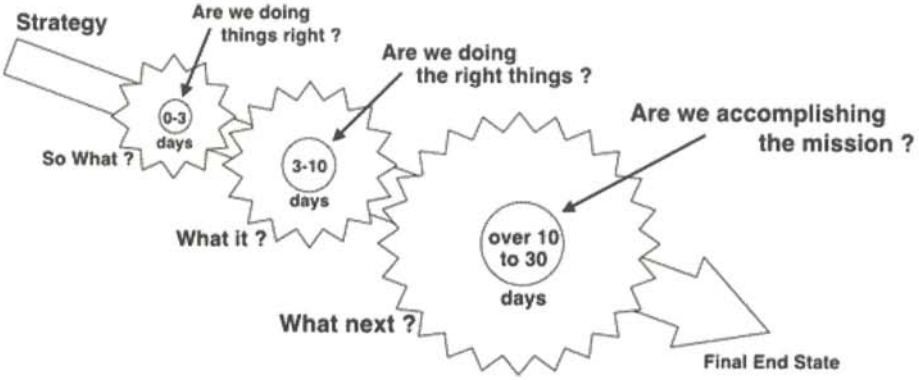
Le C2 pour gérer le « cyber »

Les dimensions de la complexité du C2 l'inscrivent dans une dynamique de création hybride, artificielle et humaine, de représentations pour la décision. C'est sur ces représentations que les acteurs fondent leur action. Le « cyber » est l'une des contraintes du C2, c'est aussi une motivation à son évolution permanente et la source de l'avancée théorique qui place l'homme dans la boucle (« *the man in the loop* ») pour la supériorité de l'action coordonnée dans un monde de plus en plus numérique. Or l'« espace cyber » semble entretenir quelques similitudes avec les domaines d'application du C2.

Le premier parallèle se fonde sur le cycle de la décision et sur les ajustements d'une boucle cybernétique associant quatre phases : la planification et la programmation (systèmes, réseaux, crypto, etc.), l'émission des ordres et des directives (cyber tasking), la supervision (situation *awareness* du cyberespace) et la conduite en temps proche du réel et, enfin, l'évaluation continue de la performance (tempo, qualité et intégrité des liaisons, pertinence des informations et des représentations). Les premiers sont du domaine du « *command* » (plan, direct) et les derniers du domaine du « *control* » (*monitor*, *assess*).

Le second parallèle est relatif à la programmation temporelle des opérations associant à la fois la performance de défense et la fiabilité des opérations. À partir d'une base théorique solide, enrichie à la fois par l'expérience et par la recherche, une doctrine permet de structurer un ensemble de procédures, maintenues actives ou « sur étagère » pour être directement disponibles dans la mise en œuvre des solutions adéquates dans les quatre phases du cycle de décision, tant pour la gestion du risque que pour le management des crises.

La culture du C2 a théorisé trois horizons temporels imbriqués qui se partagent les tâches à accomplir et la typologie de l'analyse des résultats et des effets obtenus. Le premier, à court terme, se tient prêt à réagir à l'imprévu et pose la question de la performance des actions programmées en cours : « *the things right* ». Le second envisage l'action à moyen terme et se prépare à anticiper les situations critiques ou celles qui ne sont pas conformes (« *branch plans* »). Il analyse la qualité des effets obtenus et la manière dont on y parvient : « *the right things* ». Le troisième pense les séquences opérationnelles suivantes et s'attache à évaluer la réussite de la mission.



Les 3 horizons C2 du cycle de décision.

Ces trois horizons du cycle de la décision du C2 sont applicables au « cyber » avec les objectifs généraux, avec la mise en œuvre et avec la réalisation pratique des quatre phases précédentes. Enfin, et ce n'est pas le moindre des points, le « cyber » est à la fois un espace multidimensionnel et un espace de confrontation. Naturellement inscrit dans la logique cybernétique, le « cyber » dispose des caractéristiques d'un système coordonné par le C2, dont il partage d'ailleurs les valeurs. L'hypothèse est donc celle d'un rapprochement des deux champs de la recherche et de ces deux volets complémentaires de l'exercice de Défense.

Conclusion

Les spécialistes du C2 sont chaque jour plus immergés dans le monde numérique, dans la représentation virtuelle du réel, dans la programmation et dans la gestion coordonnée pour une mobilisation de moyens au service d'une stratégie. S'ils disposent d'outils, de méthode et d'un champ pratique, ils participent à la construction d'un véritable domaine d'étude théorique, à visée applicative.

Les évolutions de ce domaine sont impactées par la préoccupation « cyber ». Mais inversement cette réflexion doit pouvoir servir au « cyber » et cela selon au moins deux pistes complémentaires : ouvrir la réflexion épistémologique du monde « cyber » sur l'opérationnel et disposer des méthodes de contrôle de l'espace virtuel du « cyber » grâce au C2, à ses principes, à ses méthodes et à ses outils.