Table des matières

Sommaire	7
Liste des sigles et acronymes	11
<i>Didier DANET, Mélanie DUBUY, Stéphane TAILLAT et Sandrine TURGIS</i>	
Introduction	13

Première partie

Enjeux et identification de la « guerre hybride »

Titre 1^{er} – Les enjeux de la « guerre hybride » : perspectives historiques et actualité d'un contexte	19

Paul CHARON

La « guerre hybride ». Mérites et démérites d'un concept équivoque	21

Stéphane TAILLAT

L'environnement international et stratégique de la « guerre hybride »	27
I. Des stratégies pour un monde incertain?	28
A. Le relâchement du monde?	29
B. Trois logiques pour les stratégies « hybrides »	30
II. Des stratégies pour un monde global, interconnecté et interdépendant?	31
A. L'arsenalisation de l'interdépendance	32
B. La subversion informationnelle	34
Conclusion : vers une refonte doctrinale?	34

Titre 2^e – Les éléments constitutifs des stratégies « hybrides » 37

Stéphane TAILLAT

Les stratégies « hybrides ».

Le retour de l'ambiguïté dans les relations internationales 39

- I. La recomposition des états de violence et de conflictualité 40
  - A. La « violence clandestine ou dispersée » et les contraintes sur la guerre ... 41
  - B. Continuum de la conflictualité et de la violence politique 42
- II. La recomposition de la grammaire stratégique 45
  - A. Les fonctions de l'ambiguïté stratégique 45
  - B. Une nouvelle grammaire stratégique ? 46
- Conclusion : effets et limites de l'ambiguïté des stratégies « hybrides » 48

Julien NOCETTI

La désinformation : au cœur des stratégies hybrides ?

Le cas de la Russie depuis 2014 49

- I. De la déstabilisation par l'information 49
- II. Vue de Russie, la « sphère informationnelle » est vectrice de menaces à circonscrire 50
- III. De la Crimée à Damas : l'évolution des pratiques informationnelles russes ... 52
- IV. Depuis février 2022, la stratégie russe s'inscrit dans la continuité des campagnes précédentes 53
- Conclusion 55

Didier DANET

Les acteurs de l'hybridité 57

- Introduction 57
- I. Les acteurs non étatiques au cœur des guerres hybrides 58
  - A. Du profiteur de guerre au mercenaire qui s'ignore, les multiples figures des acteurs privés dans les conflits contemporains 58
    - 1. Starlink, un sauveur intéressé 58
    - 2. Conti, un patriotisme quelque peu forcé ? 59
    - 3. L'IT Army, la guerre à temps partiel 60
  - B. Le problème de la gouvernance 61
- II. Quels modes de gouvernance pour les conflits hybrides ? 62
  - A. La coordination par des formes contractuelles complexes 62
  - B. Quelles modalités pratiques ? 63
    - 1. La centralisation par l'État des contributions individuelles à l'effort de défense (dimension organisationnelle) 64
    - 2. La décentralisation de certaines missions à des opérateurs privés (dimension contractuelle) 64
    - 3. La création d'une vision commune de la cyberdéfense (dimension culturelle) 65
- Conclusion 65

Seconde partie

Le cadre juridique, institutionnel et opérationnel de la « guerre hybride »

Titre 3^e – La reconnaissance des menaces « hybrides » par les organisations internationales	69

Aimoi Ninguet MOUSSODJI MATSANGA

L'intégration du concept de guerre hybride dans les stratégies sécuritaires des organisations internationales de défense et de sécurité	71
I. <i>Les approches institutionnelles du concept de guerre hybride</i>	72
A. La perspective militaire ou civile de la guerre hybride de l'OTAN et de l'UE	72
B. La perspective ambiguë de la guerre hybride de l'OSCE	75
II. <i>Le rejet d'une appropriation du concept de « guerre hybride » par la notion de « menaces hybrides »</i>	76
A. L'antagonisme stratégique et temporel de la guerre hybride et des menaces hybrides	76
B. La carence d'une nature guerrière des menaces hybrides	77

Jean Félix DELILE

La lutte contre les menaces hybrides. Esquisse de l'émergence d'une nouvelle politique de l'Union européenne	79
I. <i>La lutte contre l'incitation à la commission d'actes terroristes</i>	81
II. <i>La lutte contre la désinformation et la déstabilisation du débat démocratique</i> ...	84
III. <i>La lutte contre les cyberattaques</i>	89

Sandrine TURGIS

Le Conseil de l'Europe et la « guerre hybride »	93
I. <i>Les défis associés à l'attention portée par le Conseil de l'Europe à la « guerre hybride »</i>	94
A. De la difficulté de passer de la définition de la « guerre hybride » à la qualification d'une telle situation	95
B. Le rattachement de la « guerre hybride » aux compétences du Conseil de l'Europe	96
II. <i>La question de la pertinence de l'arsenal juridique du Conseil de l'Europe face à la « guerre hybride »</i>	97
A. La spécificité et les limites de la Convention de Budapest sur la cybercriminalité	97
B. De l'opportunité d'une convention sur les aspects non militaires de la « guerre hybride » à l'obligation de respecter les droits de l'homme ...	98
Conclusion	100

**Titre 4^e – L’encadrement juridique et opérationnel
de la « guerre hybride »** 101

Mélanie DUBUY

La guerre hybride et les règles du *jus ad bellum*.
L'impossible invocation du droit de légitime défense? 103

I. *La difficile qualification d'agression armée* 105

A. Le concept d'agression armée, élément déclencheur du droit
de légitime défense 105

B. La difficile qualification des éléments constitutifs
de la guerre hybride d'agression armée 106

1. *Premier pilier : les campagnes de désinformation* 106

2. *Deuxième pilier : la coercition économique* 108

3. *Troisième pilier : l'envoi d'hommes (war by proxy)* 108

II. *La parade : le cumul des événements* 110

A. La théorie du cumul des événements (*pinpricks doctrine*) 110

B. L'application de la théorie au cas de la guerre hybride 111

Caroline BRANDAO

L'impact de la guerre hybride sur le droit et l'action humanitaire 115

I. *Les cyberattaques* 116

A. Une attaque hautement sophistiquée et ciblée 116

B. Les auteurs de l'attaque 117

II. *Les menaces hybrides : les campagnes de désinformation* 118

A. Une campagne de désinformation massive déstabilise le CICR
en Ukraine 119

B. Burkina Faso : les conséquences humanitaires de la désinformation
au cœur d'une campagne internationale d'investigation 120

Florent FAVIÈRE

La coopération UE-OTAN comme réponse à la guerre et les menaces hybrides ... 123

I. *La structuration formelle de la coopération UE-OTAN
face à la guerre et aux menaces hybrides* 124

A. L'approche initialement distincte de l'UE et de l'OTAN 124

B. L'élaboration d'un cadre formel à la coopération entre l'UE et l'OTAN ... 126

II. *La coopération protéiforme entre l'UE et l'OTAN
face à la guerre et aux menaces hybrides* 128

A. La coopération au niveau institutionnel entre l'UE et l'OTAN
par un dialogue politique 128

B. La coopération au niveau opérationnel entre l'UE et l'OTAN
par une pluralité de vecteurs 129

1. *Le Centre d'excellence européen pour la lutte contre les menaces hybrides* ... 130

2. *La coopération en matière de connaissance de situation* 130

3. <i>Étroite collaboration dans le domaine de la communication stratégique pour lutter contre la désinformation</i>	131
4. <i>Les exercices parallèles et coordonnés dans un contexte de guerre hybride</i> ...	132

Didier DANET

Des opérations d'influence à la sécurité cognitive.	
Faire face aux menaces dans le champ informationnel	135
<i>Introduction</i>	135
I. <i>Des opérations d'information à la sécurité cognitive : anciennes et nouvelles menaces</i>	135
A. <i>L'approche occidentale de la guerre cognitive : la technologie d'abord</i> ..	135
B. <i>L'approche russe de la guerre cognitive : la désinformation d'abord</i>	136
II. <i>Menaces cognitives : un modèle</i>	136
III. <i>Organisations occidentales à risque : vulnérabilités</i>	137
IV. <i>Améliorer la sécurité cognitive dans les environnements de crise</i>	139
A. <i>La sécurité cognitive face à la dégradation de l'environnement</i>	140
B. <i>La sécurité cognitive et l'effondrement de la création de sens</i>	141
<i>Conclusion</i>	141

Lucie PAIOLA

Pertinence et limites d'un cessez-le-feu dans un contexte de « guerre hybride »	143
I. <i>La pertinence du cessez-le-feu dans un contexte de « guerre hybride » assimilée à un conflit armé</i>	145
A. <i>L'absence de pertinence d'un cessez-le-feu face à des « menaces hybrides » détachées d'un conflit armé</i>	145
B. <i>Les effets a priori limités d'un cessez-le-feu dans une « guerre hybride » assimilable à un conflit armé</i>	147
II. <i>L'adaptabilité du cessez-le-feu au phénomène de la « guerre hybride »</i>	148
A. <i>L'élasticité de la notion de cessez-le-feu</i>	148
B. <i>Les éléments additionnels et contingents du cessez-le-feu adaptables au phénomène de la « guerre hybride »</i>	149

Titre 5^e – Stratégies « hybrides » et nouvelles technologies : le cas des cyberattaques	151

Irène COUZIGOU

La qualification d'une cyberattaque. Des critères imprécis	153
I. <i>Une cyberattaque comme force armée</i>	154
A. <i>Une cyberattaque aux conséquences matérielles</i>	154
B. <i>Une cyberattaque aux conséquences immatérielles</i>	156

II. Une cyberattaque comme agression armée	158
A. Une cyberattaque aux graves conséquences matérielles ou immatérielles ...	158
B. Une cyberattaque aux contours flous	159
Aude GÉRY	
Limputation d'une cyberattaque. Un problème surestimé?	163
I. La preuve dans l'imputation des cyberattaques	164
A. La force probante des preuves : l'absence de <i>smoking gun</i>	164
B. Standards de preuve et imputation d'un acte	167
II. La qualification des relations entre individus et États : des difficultés liées aux spécificités de l'espace numérique	169
A. Limputation d'actes conduits par des acteurs non étatiques sur la base de l'article 8 AREFII	169
B. Limputation d'actes conduits par le secteur privé sur la base de l'article 5 AREFII	171
Jean-Vincent HOLEINDRE	
Conclusion. La guerre hybride, symptôme d'une crise de la guerre	175
Les auteurs	181