EUROPEAN FOREIGN POLICY IN 2027: PREPARING FOR THE UNEXPECTED

RISKS AND MITIGATION APPROACHES

Zukunftsdialog 2017

February 2018

[12th February 2018 at 23:51 – version *459e74d*]

Zukunftsdialog 2017: *European Foreign Policy in 2027: Preparing for the Unexpected*, Risks and Mitigation Approaches,

[12th February 2018 at 23:51 – version *459e74d*]

CONTENTS

cleardoublepage

PRÉFACE

À quels risques l'Union européenne (UE) pourrait-elle faire face en 2027? Secoué par agitation interne croissante ainsi que des développements géopolitiques plus larges l'UE doit redéfinir son rôle sur la scène mondiale tout en renforçant son projet de base. L'intégration a eu lieu à tous les niveaux et risques sont donc de plus en plus une préoccupation pour l'UE dans son ensemble. Le Lisbonne Le traité a établi plusieurs instruments pour renforcer et coordonner son action extérieure en 2009. Cette politique est toutefois confrontée sérieux défis internes et externes qui remettent en question sa capacité à définir et défendre un intérêt européen à long terme. Les décideurs politiques de l'UE Il faut donc analyser les risques et prendre des mesures de précaution.

Dans ce rapport, un groupe de 30 jeunes Allemands, Français et Polonais avec divers milieux professionnels présentent des scénarios sur les risques majeurs menacer les intérêts de la politique étrangère de l'UE.

Les scénarios ignorent inévitablement de nombreux risques difficiles, soit parce que les décideurs les ont déjà considérés, ou parce que les participants évalué leur signification trop hétérogène. Un des principaux défis a été d'observer les signaux faibles, en ce qui concerne les menaces réelles encore moins connu, moins étudié ou risque de faire partie de notre quotidien la vie, que nous ne parvenons pas à les percevoir.

Certains scénarios (par exemple «guerre contre le sable») ont également surmonté notre capacité d'expertise et exigerait une compréhension plus profonde. De plus, étudier les possibles les interactions entre les scénarios montre que les risques de conduite comme les données la manipulation ou la pénurie de ressources sont des développements lents dans le besoin de surveillance constante. À l'autre extrémité du spectre, les scénarios construits sur la montée du populisme semblent être favorisés par d'autres scénarios les populistes pourraient exploiter tous les impacts négatifs sur les politique.

Dans un monde de (fausses) nouvelles, un combat pour la vérité semble donc émergent: les auteurs appellent à un engagement fort de l'UE et de ses États membres pour plus de transparence et une meilleure communication afin de (re) renforcer la confiance entre ses citoyens et envers les institutions. Cela constitue une condition préalable essentielle à la rédaction de la résilience de l'UE stratégies de surveillance, de prévention et d'intervention d'urgence les cinq principaux risques identifiés dans ce qui suit. Ce faisant, l'UE renforcera sa capa-

1 CYBER-ATTAQUES SUR L'INFRASTRUCTURE EUROPÉENNE

1.1 DÉFINITION

Une cyber-attaque peut être une manœuvre offensive ciblant les TI systèmes informatiques, réseaux informatiques et ordinateurs personnels par divers moyens de actes malveillants, provenant généralement d'une source anonyme. Comme les réseaux se sont répandus dans nos vies quotidiennes, les cyberattaques peuvent être déployées par des États-nations, des organisations criminelles, des groupes ou personnes. Ils peuvent ainsi être qualifiés de cyber-campagne, cyber-guerre ou cyber-terrorisme en fonction du contexte.

1.2 IMPACTS POTENTIELS ET CONSÉQUENCES

- Les cyber-attaques entraînent une série de problèmes, de la manipulation de l'informatique affectant les infrastructures, à la perte de leadership et de réputation, capacité réduite à agir, diplomatique, économique et humanitaire crises et ainsi de suite.
- La cyberguerre dirigée par l'État cible les infrastructures, en particulier il permet d'avoir un impact sur la vie de millions de personnes avec seulement ressources limitées.
- Systèmes de contrôle industriel, infrastructures énergétiques et financières, les télécommunications, les transports et les infrastructures de l'eau apparaissent comme une cible de choix pour le cyber-terrorisme et la cyber-guerre dans général.

1.3 SCÉNARIO

[L'UE est frappée par le piratage de l'apocalypse du système financier. Jeu terminé pour l'UE économie?] {. soulignement}

Le 1er janvier 2025 aurait dû marquer la percée finale sur le chemin de États-Unis d'Europe et était censé compléter le union bancaire. Cependant, des cyberattaques sans précédent sur le plan financier les marchés ont causé des ravages dans toute l'Europe, et mis son avenir économique en peril. Des nationalisations hâtives et non coordonnées n'ont pas empêché crise économique qui s'ensuit et les dirigeants politiques sont toujours en désaccord sur comment gagner cette guerre et contre qui.

Comme nous le disent les cyber-experts, cette crise a duré des décennies: le marché unique numérique conduit à une société presque sans numéraire; chaîne de bloc transferts fondés sont devenus une partie

fondamentale de notre économie et de notre vie quotidienne. La majorité des actifs sont gérés par des algorithmes à travers progrès rapides dans la recherche d'intelligence artificielle (A.I.). Une augmentation dans les capacités de cyber-guerre conduire en même temps à un grand niveau de Vulnérabilités grandement sous-estimées

Les vraies origines de cette crise sont encore enveloppées de brume. Quels leaders prétendre savoir, c'est qu'une grande puissance étrangère a infiltré les services bancaires de l'UE réseaux et confus des fonds dirigés par A.I. et les investisseurs avec des données altérées. Cela a provoqué des éruptions de mouvements de vente et d'achat suicidaires qui ont ruiné un acteur financier après l'autre et la perte de confiance généralisée conduit à des courses de banque. Le système financier européen s'effondre.

Au sein de l'UE, la crise a rapidement dégénéré en un cascade de réactions nationalistes. Une réponse coordonnée et conjointe à Le niveau de l'UE est désespérément manquant, de même que la solidarité en Europe.

1.4 RECOMMANDATIONS POLITIQUES

Tous les systèmes informatiques critiques - publics ou privés - doivent être redondants, décentralisé et crypté afin d'améliorer leur résilience contre cyber-attaques. Les administrations doivent développer l'analogique et le déconnecté plans de sauvegarde et expertise défensive en matière de guerre cybernétique en général.

Nous avons besoin d'une coopération plus étroite entre les acteurs publics et privés au niveau de l'UE combiner la flexibilité du secteur privé avec les droits légaux autorité. Nous devons améliorer les canaux de communication et encourager procédures communes.

Nous avons besoin de méthodes de transaction financière alternatives pour éviter la dépendance systèmes traditionnels et d'atténuer l'impact d'éventuelles perturbations.

Les acteurs privés et publics ont besoin de moderniser et d'améliorer globalement capacités de cyber-guerre. Ceci est particulièrement important dans la clé environnements économiques, comme le secteur financier où intelligent 'tripwires' dans les algorithmes financiers devrait déclencher l'arrêt d'urgence.

Nous avons besoin du leadership de l'UE pour cette législation. Cela renforcerait l'UE dans son ensemble.

2 HAUSSE DU POPULISME DANS LES ETATS MEMBRES DE L'UE

2.1 DÉFINITION

Le populisme peut prendre diverses formes, mais fonctionne toujours sur la base d'un concept de base, les * personnes *, considérées comme un collectif homogène et servir à la fois de source et de destinataire des actions politiques. UNE élément central est la différenciation des autres: des 'élites' et l'établissement d'un côté, ainsi que d'autres peuples, nations et donc les immigrants de l'autre. Ceci est également lié à un crise de la démocratie représentative. Les citoyens ont l'impression que leurs intérêts ne sont plus représentés.

2.2 IMPACTS POTENTIELS ET CONSÉQUENCES

- L'euroscepticisme et le populisme se développent en raison d'une perte de confiance dans la politique structures et se manifestent par des résultats électoraux. Médias la fragmentation, la polarisation à travers les réseaux sociaux et les fausses nouvelles faciliter davantage ce développement.
- Les gouvernements se concentrent sur les questions nationales - et les mentalités changeantes et les programmes politiques des partis établis afin de gagner électeurs populistes - conduisent à un cercle vicieux.
- L'UE perd

AUTHORS

The following participants of the Zukunftsdialog 2018 have contributed to this report:

Marysabelle Cote, Vivien Croes, Jakobine von Freytag Loringhoven, Corinne Kowalski, Benjamin Kurc, Sophie Pornschlegel, Lorraine Puzin, Jean Michel Romano, Chloé Saby, Charles Thépaut, Daniela Heimpel, Hendrik Herkert, Kristina Karnahl, Klemens Kober, Nina Ohlmeier, Raphael Rauch, Robert Riemann, Max Schulze, Cara Catharina Stauss, Malwina Ewa Kołodziejczak, Aneta Krzyworzeka-Jelinowska, Jacek Kubera, Agnieszka Lichnerowiocz, Hanna Luczkievicz, Maia Mazurkiewicz, Katarzyna Nowicka, Adam Konrad Puchejda, Pawel Zerka

http://zukunftsdialog.eu/

COLOPHON

This document was typeset with XeLaTeX using the typographical look-and-feel `classicthesis` developed by André Miede and Ivo Pletikosić. The style was inspired by Robert Bringhurst's seminal book on typography "*The Elements of Typographic Style*". `classicthesis` is available for both LaTeX and LyX:

https://bitbucket.org/amiede/classicthesis/

Hermann Zapf's *Palatino* and *Euler* type faces (Type 1 PostScript fonts *URW Palladio L* and *FPL*) are used. The "typewriter" text is typeset in *Bera Mono*, originally developed by Bitstream, Inc. as "Bitstream Vera". (Type 1 PostScript fonts were made available by Malte Rosenau and Ulrich Dirr.)