Mémoire de stage : Institut français d'Estonie / Service de coopération et d'action culturelle, ambassade de France à Tallinn.

Université Paris Nanterre
UFR Langues et cultures étrangères
Master 2 en études russes et post-soviétiques

Sous la direction de Jean-Robert Raviot
Maître de stage : Ulla Kihva

Juin 2023

Paul du Rosel de Saint Germain

Remerciements

Mes remerciements se dirigent tout d'abord vers mes collègues de l'Institut français d'Estonie, du service de coopération et d'action culturelle de l'ambassade de France à Tallinn et des autres services de l'ambassade, particulièrement de la mission défense. Je pense particulièrement à Eric Bultel, Dora Catheline, Ulla Kihva, Danaë di Salvo, et Mélie Cornet qui ont rendu ce stage possible et particulièrement agréable grâce à la variété des missions proposées.

Je remercie également mon directeur de master et de mémoire Monsieur Jean-Robert Raviot, ainsi que Kevin Limonier et tous les professeurs du master Études russes et post-soviétiques de l'université Paris-Nanterre pour leurs enseignements de grande qualité.

Enfin, j'ai aussi une pensée pour mes camarades de classe, mon équipe de rugby à Tallinn, le Kalev RFC, ainsi que pour Son Excellence l'ambassadeur de Moldavie Ion Stavila.

Sommaire

Prologue

Le choix de ce sujet de mémoire de stage fut l'objet d'une réflexion de plusieurs semaines. En effet, bien que mon stage ait été particulièrement intéressant et enrichissant sous tout aspect, la problématisation de celui-ci et l'identification d'un axe de développement restaient difficiles à établir.

De plus, le stage en lui-même était assez décorrélé avec mon projet professionnel, mais grâce à sa situation géographique il me fut possible d'établir une cohérence avec mon espace d'étude et le profil que je souhaite présenter. Par ailleurs, la destination de l'Estonie présente l'intérêt de me donner une expérience de vie dans le seul pays Balte que je n'avais pas encore pu visiter.

En conséquence, bien que n'ayant pas de sujet de mémoire en tête, j'ai profité de mon expérience pour saisir les opportunités qu'offrait un stage en ambassade pour découvrir le pays sous ses nombreux aspects, qu'ils soient culturels, stratégique, diplomatique, militaire, linguistique ou autres, en espérant mettre le doigt sur le thème qui ferait l'objet d'un développement.

La démarche fut payante, et après un délai de réflexion assez important, je décidais d'aborder l'Estonie sous son aspect le plus significatif : le numérique. Et pour faire le lien avec mon stage, car la est l'objectif de ce travail, je décidais de m'inspirer de ma contribution à une note à l'intention de Son Excellence l'ambassadeur : La guerre en Ukraine : un laboratoire des conflictualités cyber pour l'Estonie.

Pour résumer, ce travail ne répond pas à la problématisation de mon expérience à l'ambassade de France à Tallinn comme stagiaire de l'Institut français d'Estonie, mais à celle d'une mission confiée lors de ce séjour.

Abréviations

OTAN : Traité de l'Atlantique Nord.

UE : Union Européenne.

CCDCOE : *Cooperative Cyber Defence Centre of Excellence* - Centre d'excellence pour la cyberdéfense en coopération.

DDoS : *Distributed Denial-of-Service* - Attaque par dénis de service

RuNet : *Russian Network* - Internet russophone.

ONU : Organisation des Nations Unis.

UAF : *Ukrainian Armed Forces* - Forces armées ukrainiennes.

eGA : *e-Governance Academy*.

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information.

RIA : *Riigi Infosüsteemi Amet* - Autorité nationale des systèmes d'information.

MKM : *Majandus- ja Kommunikatsiooniministeerium* - Ministère de l'économie et de la communication.

ERR : *Eesti Rahvusringhääling* - Radio télévision publique estonienne.

URSS : Union des Républiques Socialistes Soviétiques.

TIC : Technologies de l'Information et de la Communication.

COMCYBER : Commandement de la Cyberdéfense.

PIB : Produit Intérieur Brut.

MoU : *Memorandum of Understanding in the field of Digital Transformation*.

L'Estonie, Cyber-poids lourd européen

Introduction :

Il est important de savoir que dans l'esprit des estoniens les cyberattaques russes de 2007 n'ont pas été une occasion de décréter que la numérisation des services gouvernementaux était trop dangereuse, mais au contraire une façon d'identifier une fragilité et d'agir en conséquence en investissant dans la cybersécurité pour conserver ce modèle. Voilà les termes par lesquels Claudia Scherer-Effosse, ambassadrice de France en Estonie (2016-2019), dont j'ai à de nombreuse reprise croisé le portrait dans l'escalier de l'ambassade, définit le rapport des estoniens à leur e-gouvernement et leur cybersécurité à l'occasion d'une conférence pour les alumnis Arts & Métiers en avril 2018[1]. Il s'agit là d'une bonne manière d'aborder l'approche estonienne du monde numérique et de poser une affirmation qui sera développée plus tard dans ce travail, l'Estonie est un cyber-Etat.

Dans ce travail nous expliquerons la construction de l'Estonie comme nation numérique incontournable et le rôle que le pays joue sur le plan international grâce à son expertise dans ce domaine principalement dans le contexte de la guerre en Ukraine. Cependant nous n'approfondirons pas le détail des offensives cyber que peuvent lancer les estoniens ou la manière exacte dont ils coopèrent avec l'Ukraine et ses alliés pour contrer les attaques russes.

[1] Arts & Métiers Alumni, E-gouvernement et menace cyber : le cas de l'Estonie, s.l., s.n., 2018.

Pour remettre ce mémoire de stage dans le contexte actuel, enfonçons tout de suite une porte ouverte : la guerre en Ukraine. Depuis le 24 février 2022, l'Estonie est en première ligne du soutiens à l'U kraine ; il ne se passe pas une journée sans qu'une actualité liée de près ou de loin à la guerre en Ukraine n'apparaissent sur le site d'ERR[2], le plus grand média du pays. Partout, les Estoniens passent devant les drapeaux du pays envahi, particulièrement celui immense de Vabaduse väljak, la place de la liberté, la plus importante du pays. Nous reviendrons plus en détail sur le soutiens estonien à l'Ukraine, mais pour remettre les choses en perspective et démontrer un peu plus la manière dont le pays vie la crise de manière quotidienne sur son sol, il faut rappeler que l'Estonie accueil actuellement 69 616 réfugiés ukrainiens[3] représentant un groupe équivalent à 5.27% de la population du pays. Pour remettre ce chiffre en perspective, en Pologne, pays qui accueil le plus de réfugiés d'Ukraine à savoir 1.5 millions[4], cette population représente 3.62% des habitants. Et en France, où nous accueillons 119 000 réfugiés[5], ces derniers ne représentent que 0.17% de la population. La contribution estonienne et son rapport à la réalité de cette guerre sont sans commune mesure.
Pour compléter le tour d'horizon du contexte dans lequel intervient ce travail, il est aussi bon de rappeler que l'Estonie est un voisin direct de la Russie, et qu'elle compte dans sa population 322 700 russes ethniques (soit 22% des estoniens) dont 90 000 ont la citoyenneté russe[6].

Dans ce contexte de guerre ouverte et internationale avec le pouvoir du Kremlin et renforcée par un passif houleux avec le géant de l'Est, comment l'Estonie s'est t- elle construite comme pays incontournable du monde cyber et quel rôle joue-t-elle exactement face à la Russie ?

[2] ERR, News, https://news.err.ee/
[3] Ukrainian refugees by country 2023, https://www.statista.com/statistics/1312584/ukrainian-refugees-by-country/
[4] Ukrainian refugees by country 2023, https://www.statista.com/statistics/1312584/ukrainian-refugees-by-country/
[5] Ukrainian refugees by country 2023, https://www.statista.com/statistics/1312584/ukrainian-refugees-by-country/
[6] Russian minority in Estonia turns its back on Putin, https://www.euractiv.com/section/politics/short_news/russian-minority-in-estonia-turns-its-back-on-putin/ , 23 mars 2022.

Pour réaliser ce travail je me suis principalement appuyé sur les informations disponibles en source ouverte, sur mes observations et mon expérience personnelle, notamment mes rencontres et discussions avec les Estoniens, ainsi que sur l'expertise de ma collègue attachée de coopération numérique à l'ambassade de France à Tallinn.

Dans le développement qui suit, sera présentée dans un premier temps la nation numérique estonienne, avec d'abord le pari placé sur ce domaine, puis les cyberattaques russes de 2007. Dans un second temps sera abordée la place de l'Estonie dans la cyberdéfense de l'OTAN, avec un focus sur centre de cyberdéfense de l'organisation et les exercices internationaux qui y ont lieu. Enfin dans une dernière partie sera décrit le rôle de l'Estonie comme fer de lance du soutien à l'Ukraine, premièrement comme leader d'une coalition internationale et deuxièmement sous l'angle de l'étroite coopération entre les deux nations.

CHAPITRE I - La nation numérique estonienne

SECTION A - Le pari du numérique

Les circonstances historiques, combinées à une vision politique ambitieuse, ont permis à l'Estonie de monter dans le train du numérique. Le pays a saisi les opportunités offertes par les nouvelles technologies, a investi dans les infrastructures numériques et a développé un écosystème favorable à l'innovation. Cela a contribué à l'émergence de l'Estonie en tant que puissance reconnue dans le domaine du numérique.

1 - Construire à partir de rien

Parti de rien? En réalité pas vraiment, l'Estonie avait déjà une culture du cybernétique et de la technologie. Avant l'indépendance, l'Union soviétique avait développé une expertise en matière d'informatique en Estonie[7], et de nombreuses entreprises technologiques étaient déjà présentes dans le pays, fournissant une base solide sur laquelle le pays a construit son avenir numérique.

[7] Gaskell Adi, How Estonia Became The Digital Leader Of Europe, https://www.forbes.com/sites/adigaskell/2017/06/23/how-estonia-became-the-digital-leaders-of-europe/.

Après l'indépendance en 1991, le pays s'est trouvé dans une position unique pour repenser le fonctionnement de l'administration et intégrer les nouvelles technologies. L'effondrement de l'URSS a forcé l'Estonie a reconstruire ses institutions et son infrastructure à partir de zéro. Ce processus a été une opportunité pour le pays de se débarrasser de la bureaucratie soviétique et de repartir sur de nouvelles bases en tirant parti de l'émergence des technologies de l'information et de la communication pour moderniser l'administration publique et améliorer la vie des citoyens avec des avantages concrets tels que l'efficacité, la transparence et la facilité d'accès aux services publics[8].

En conséquence, le gouvernement estonien a adopté une approche proactive pour promouvoir le secteur des TIC et a mis en place des politiques favorables aux start-up technologiques, encouragé l'investissement dans les infrastructures numériques et lancé des programmes de formation pour développer les compétences numériques de la population[9].

2 - Les politiques fondatrices

Les décisions politiques estoniennes permettant la mise en place de cette société numérique se concrétisent à travers deux grands piliers posés en 1994 et 1996, et qui aboutiront en 2002 sur la carte d'identité et la signature numérique.

[8] Européennes : comment la petite Estonie est devenue le royaume du tout-numérique et de l'e-administration, https://www.tf1info.fr/high-tech/elections-europeennes-2019-comment-l-estonie-est-devenue-le-royaume-du-tout-numerique-et-de-l-e-administration-2122042.html , 24 mai 2019.
[9] *How it all began? From Tiger Leap to digital society*, https://www.educationestonia.org/tiger-leap/.

En 1994 commence l'élaboration des Principes de la politique d'information estonienne[10], le plan stratégique de développement informatique servant de base à la construction du pays qui sera ratifié 4 ans plus tard. Le texte comprend 30 principes regroupés en 8 chapitres, mais nous pouvons en retenir 5 principaux : L'Estonie s'engage à garantir l'accès équitable aux services numériques pour tous les citoyens. L'Estonie reconnaît l'importance de la confidentialité et de la sécurité des données personnelles dans un environnement numérique. L'interopérabilité des systèmes d'information est un principe clé de la politique de l'information estonienne. L'Estonie promeut la collaboration et la coopération entre les secteurs public et privé, ainsi qu'entre les différentes parties prenantes de l'écosystème numérique. La prise en compte des aspects sociaux et environnementaux dans la conception et la mise en œuvre des solutions technologiques.

Le saut du tigre (*Tiigrihüpe*) est un projet du gouvernement estonien qui intervient en 1996 dans la suite logique des politiques entamées en 1994. Son objectif était de moderniser l'administration publique, d'améliorer les services en ligne et de promouvoir l'utilisation des technologies numériques principalement à l'école[11]. Il a permis la mise en place d'infrastructures technologiques, l'intégration des TIC dans l'éducation dès le plus jeune âge en permettant en seulement 3 ans de doter toutes les écoles du pays d'un accès internet[12], le développement de l'e-gouvernement et l'encouragement de l'innovation technologique. Grâce au saut du tigre, l'Estonie est devenue un exemple mondial en matière de gouvernance numérique et a attiré l'attention internationale. Ce programme a joué un rôle clé dans la création d'une société de l'information avancée en Estonie, offrant des services en ligne aux citoyens et favorisant le développement d'une économie numérique dynamique.

SECTION B - Les cyberattaques russes de 2007

[10] Principles of Estonian Information Policy, https://ega.ee/publication/principles-of-estonian-information-policy/.
[11] Tiigrihüpe, https://kompass.harno.ee/tiigrihupe/.
[12] L'Estonie, pays pilote de l'Internet, https://www.latribune.fr/archives/2004/entreprises/communication/id7aa7bbacce3b8e05c1256e860045a9e4/lestonie-pays-pilote-de-linternet.html , 19 octobre 2008.

Événement déterminant dans le développement de la cyberdéfense estonienne, les cyberattaques russent qui surviennent à partir du 27 avril 2007 suite à la décision en 2006 de déplacer la statue du soldat de bronze, monument soviétique en hommage au soldats morts pendant la seconde guerre mondiale perçu par les estoniens comme un symbole de l'occupation, dans un cimetière aux abord de la ville provoquant de vives réactions en Russie[13] et jouant un grand rôle dans les élections estoniennes[14].

1 - 22 jours en enfer

Les cyberattaques ont commencé par des attaques DDoS massives, qui ont paralysé les sites gouvernementaux, les banques, les médias et les entreprises estoniennes avec un nombre de requêtes gigantesque engendrant un trafic excessif et rendant les sites inaccessibles. Les attaquants ont également utilisé des techniques plus sophistiquées, telles que l'infiltration de sites web et la diffusion de logiciels malveillants. Des groupes de hackers russes vraisemblablement soutenus par leur gouvernement[15], ont été identifiés comme étant à l'origine de ces attaques, bien que la responsabilité officielle de la Russie n'ait jamais été confirmée. Les infrastructures critiques, telles que les services bancaires et gouvernementaux, ont été sérieusement affectées. De plus, les communications et les transports ayant été touchés, les Estoniens se sont retrouvés coupés du reste du monde. Enfin, les attaques ont engendré une grande inquiétude quant à la sécurité des données personnelles des citoyens et de celles encore plus sensibles du gouvernement.

---

[13] Soldat de bronze: la Russie soulèvera la question sur la situation en Estonie au Conseil de l'Europe | International | RIA Novosti, https://archive.wikiwix.com/cache/index2.php?url=http%3A%2F%2Ffr.rian.ru%2Ftrend%2Fdemontage_talinn%2F#federation=archive.wikiwix.com&tab=url.

[14] CHALVIN Antoine, « L'ombre du soldat de bronze », in *Le Courrier des pays de l'Est*, n° 4, vol. 1062, 2007, p. 6-16.

[15] *Authoritatively, Who Was Behind The Estonian Attacks? - Hacked Off - Dark Reading*, https://web.archive.org/web/20090701212951/http://www.darkreading.com/blog/archives/2009/03/authoritatively.html , 1 juillet 2009.

Les cyberattaques de 2007 ont révélé la vulnérabilité des pays face aux menaces numériques, d'autant plus lorsqu'ils sont très développés dans ce domaine, offrant une plus grande prise à ce genre d'attaques[16], et ont incité l'Estonie à renforcer sa cybersécurité et à devenir un leader mondial dans ce domaine.

2 - La ligue de cyberdéfense

Suite à cette vague d'attaques, l'Estonie a pris un certain nombre de décisions politiques déterminantes pour renforcer sa résilience numérique et ses défenses face aux cybermenaces[17].

Ces mesures entraînent un renforcement de la législation, une amélioration de la coopération internationale, un investissement massif dans la cybersécurité, une sensibilisation et une éducation aux menaces cyber, et un renforcement des capacités de défense numérique avec notamment la création de la ligue de cyberdéfense en 2008.

La ligue est composée de civils estoniens, qu'ils soient étudiants, professionnels de l'informatique, ingénieurs ou passionnés de technologie. Ces membres volontaires sont recrutés pour leurs compétences en matière de cybersécurité et de défense numérique. Ils participent à des formations, à des exercices et à des missions pour renforcer les capacités de défense du pays dans le domaine numérique.

La ligue de cyber défense fonctionne en étroite collaboration avec les autorités estoniennes compétentes, notamment le Centre estonien des opérations de cyberdéfense et le Commandement des Forces de défense estoniennes. Elle joue un rôle important dans la surveillance des menaces en ligne, la détection des attaques, la réaction aux incidents et la sensibilisation du public à la cybersécurité.

Ses cinq missions principales sont de développer la coopération entre informaticiens bénévoles qualifiés, augmenter le niveau de cybersécurité des infrastructures d'information critiques, la création d'un réseau qui facilite le partenariat public-privé et améliore la capacité à opérer en situation de crise, l'éducation et la formation en

[16] https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[17] CCDCOE, https://ccdcoe.org/library/publications/estonia-after-the-2007-cyber-attacks-legal-strategic-and-organisational-changes-in-cyber-security/ .

sécurité de l'information et enfin la participation à des événements internationaux de formation en cybersécurité.

CHAPITRE II - La place de l'Estonie dans la cyberdéfense de l'OTAN

SECTION A - Le centre de cyberdéfense de l'OTAN

Le CCDCOE est une institution internationale basée en Estonie qui se consacre à la recherche, à l'éducation et à la coopération dans le domaine de la cybersécurité. Directement liés à l'OTAN, il bénéficie tout de même d'un statut juridique distinct[18]. Il a pour mission principale de renforcer la défense collective de l'OTAN contre les menaces cyber en menant des programmes de recherche, en sensibilisant et formant des professionnels, en coopérant avec d'autres organisations et surtout en organisant des exercices.

1 - Pourquoi l'Estonie ?

Plusieurs facteurs ont amené l'OTAN à choisir l'Estonie pour implanter son centre de cyberdéfense.

La première raison est avant tout pragmatique, en effet particulièrement développée sur le plan numérique, l'Estonie disposait déjà de toutes les infrastructures technologiques nécessaires et des ressources pour soutenir le centre et ses activités. Par ailleurs, dès 2008 les estoniens sont reconnus pour leur expertise en matière de cybersécurité en grande partie due aux attaques russes de 2007 permettant au pays de gagner en expérience et en compétence dans ce domaine avec une approche proactive de la cyberdéfense.

De plus, dès son adhésion à l'OTAN en 2004 le pays se montre très actif dans l'alliance en contribuant aux déploiements de l'alliance notamment en Afghanistan. Mais l'Estonie n'a pas attendu 2004 pour contribuer aux missions de l'OTAN, en effet on peut retrouver les forces estoniennes engagées au Kosovo dès 1999[19].

[18] NATO, Cyberdéfense, https://www.nato.int/cps/fr/natohq/topics_78170.htm .
[19] EATA | Missions and operations, https://www.eata.ee/en/nato/missions-and-operations/ .

Par ailleurs, l'Estonie s'est toujours montrée proactive dans les coopération internationale autour des questions de cybersécurité, partageant son expertise avec des pays membres de l'OTAN. Tous ces éléments démontrent l'engagement du pays pour la sécurité internationale et sa volonté de jouer un rôle actif au sein de l'alliance.
Enfin, sa situation géographique stratégique aux limites de l'OTAN et à la frontière de la Russie en font un emplacement de choix pour surveiller les menaces cybernétiques provenant de l'Est.

2 - Eduquer les pays membres

Membre de l'alliance depuis 2004 l'Estonie, forte de sa culture numérique et de son expérience en matière de cybersécurité a toujours collaboré activement dans ce domaine notamment au groupe de travail sur la politique de cybersécurité créé en 2002. C'est aussi l'Estonie qui pose les bases des politiques et des normes pour la cyberdéfense de l'OTAN[20].
L'Estonie a participé à des échanges internationaux d'informations et de bonnes pratiques en matière de cybersécurité. Elle a partagé son expertise et ses expériences avec d'autres pays, notamment lors de conférences et de séminaires internationaux. Cela a contribué à renforcer la sensibilisation et la compréhension mutuelle des défis liés à la cybersécurité. Le pays a également développé des partenariats bilatéraux dans le domaine de la cybersécurité. Par exemple, elle a coopéré avec les États-Unis dans le cadre de l'initiative du Cyber Defense Capability Building Program[21], qui vise à renforcer les capacités de cybersécurité des pays partenaires. L'Estonie a fourni une assistance technique et des conseils dans le renforcement des capacités de cybersécurité d'autres pays.

[20]https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en
[21] Kaspersky Transparency Center | Kaspersky, https://www.kaspersky.com/capacity-building .

Mais plus que tout, dans le domaine de la cybersécurité, la coopération et l'éducation se fait au travers d'exercices et de simulations visant à tester et à améliorer la préparation des pays en cas d'attaques cybernétiques. L'Estonie participe activement à tous ces exercices organisés par le Centre d'excellence de la cyberdéfense coopérative de l'OTAN[22], qui simule des scénarios réalistes d'attaques et permet aux participants de renforcer leurs capacités de défense.

SECTION B - L'organisation des exercices de cyberdéfense

La cyberdéfense est un domaine particulièrement important dans lequel l'OTAN cherche à se développer et à se renforcer. Depuis le sommet de Varsovie en 2016[23] l'organisation suit une feuille de route destinée à renforcer ses défenses. 6 ans plus tard, l'année 2022 était au sein de l'OTAN véritablement placée sous le signe de la cyberdéfense. En effet, dans un contexte de guerre multidimensionnelle en Ukraine s'est tenu à Madrid le sommet de l'OTAN au cours duquel les cybermenaces trônaient au centre des concepts stratégique pour l'année en cours[24], précédant de quelques mois la conférence 2022 de l'OTAN sur les engagements en matière de cyberdéfense[25], introduction à l'exercice Cyber Coalition 2022.

1 - Cyber coalition 2022

Cyber Coalition est un exercice annuel organisé depuis 2008 dans différents pays hôtes. La dernière édition à eu lieu en Estonie pour la 3ème fois de son histoire, ce qui est assez unique et démontre le poids du pays dans ce domaine. Il présente aussi l'intérêt de pouvoir se dérouler à distance. L'édition 2022 a regroupé 1000 participants de 26 nations alliés, 6 autres pays partenaires plus la Corée du sud comme observateur ainsi que plusieurs acteurs industriels, académiques et organismes de cyber défense[26].

---

[22] *Exercises*, https://ccdcoe.org/exercises/ .
[23] NATO, Warsaw Summit Communiqué issued by NATO Heads of State and Government (2016), https://www.nato.int/cps/en/natohq/official_texts_133169.htm .
[24] NATO, 2022 NATO Summit, https://www.nato.int/cps/en/natohq/news_196144.htm .
[25] Italy U. S. Mission, NATO's 2022 Cyber Defense Pledge Conference, https://it.usembassy.gov/natos-2022-cyber-defense-pledge-conference/ , 9 novembre 2022.
[26] Exercise Cyber Coalition 2022, https://shape.nato.int/news-releases/exercise-cyber-coalition-2022-.aspx .

L'objectif de l'exercice cette année-là[27] était de pouvoir rapidement augmenter ses capacités de défense pour protéger ses outils de communications dans un scénario ou la cyber attaque surviendrait dans les 24 heures suivantes.

La France a pu envoyer des militaires du COMCYBER mais aussi d'organismes civils[28] pour prendre part à ce scénario qui s'articule autour de plusieurs attaques cyber découvertes dans l'ensemble des milieux - terre, air, mer - à la fois sur un théâtre d'opérations extérieures et sur le territoire national. Il comprend des attaques d'infrastructures critiques, des intrusions dans les réseaux, l'exfiltration ou encore la manipulation de données sensibles et permet d'exercer une capacité militaire de lutte informatique défensive à partir de tactiques, techniques et procédures de cyberdéfense sur des réseaux militaires de circonstances et d'infrastructures simulés.

Chaque action à mener est d'abord soumise au cadre légal des opérations dans le cyberespace. Cyber Coalition permet donc aussi de contribuer au dialogue de la communauté juridique de cyberdéfense, le tout en communiquant en temps réel sur les menaces avec les partenaires de l'alliance comme l'Union Européenne.

En plus de travailler à bâtir une défense collective efficace, les pays membres sont appelés à investir dans l'interopérabilité avec les alliés de la cyberforce face notamment à des *challengers* comme la Russie et la Chine[29].

Ce genre d'exercice est organisé sur un modèle de confrontation *Blue team* contre *Red team*, en d'autres termes une équipe de défenseur qui protège les objectifs tandis que l'équipe attaquante tente de s'infiltrer pour causer des dégâts, entraver la coopération des défenseurs et récolter des informations sensibles.

2 - Locked Shield

A l'image de Cyber Coalition, Locked Shields est un exercice annuel. Cependant si Cyber Coalition est un exercice de l'OTAN à l'hôte variant d'une année sur l'autre, Locked

[27] NATO MILITARY SHAPE, Cyber Coalition 2022, NATO's flagship cyber defence exercise, s.l., s.n., 2022.
[28] Le COMCYBER participe à CYBER COALITION 2022, exercice international de grande envergure de l'OTAN | Ministère des Armées, https://www.defense.gouv.fr/ema/actualites/comcyber-participe-cyber-coalition-2022-exercice-international-grande-envergure-lotan , 9 décembre 2022.
[29] NATO PA, https://www.nato-pa.int/document/2022-offence-defence-natos-cyber-challenge-report-pinotti-015-dscfc , 23 juin 2023.

Shields est organisé en Estonie par le CCDCOE depuis 2010 et l'éventail de participants est bien plus large car il n'est pas réservé aux seuls membres de l'OTAN[30]. L'édition 2023 est le plus grand exercice de cybersécurité interallié jamais réalisé au niveau mondial, regroupant plus de 2000 participants, permettant de mesurer la crédibilité de l'Estonie dans le domaine.

Pour parler de Locked Shields il convient de comparer avec Cyber Coalition que nous avons introduit juste avant. L'exercice Cyber Coalition se déroule généralement dans un format de simulation, où les participants sont confrontés à des scénarios de cyberattaques et doivent coordonner leurs réponses et leurs actions. Cependant, l'exercice Locked Shields est un exercice en temps réel, où les équipes de défense cybernétique doivent réagir en direct à des attaques simulées. Cela permet de tester les capacités techniques, les processus de collaboration et les protocoles de communication des participants dans des conditions proches de la réalité.
Les deux exercices se ressemblent sous beaucoup d'aspects, notamment à travers le modèle *Blue team* contre *Red team* (bien que pour Locked Shields l'équipe de défense soit la *Green team*). Mais pour l'édition 2023 de Locked Shields intervient une innovation particulière, la *White team*, équipes dédiées à la gestion des problématiques juridiques, médiatiques et diplomatiques au cœur de l'exercice. D'ordinaire dans les exercices similaire possèdent aussi une équipe blanche mais elle est généralement dédiée à la coordination et la gestion de l'exercice, la ou ce role est remplit par une équipe Jaune dans le cas Locked Shields.

[30] Locked Shields, https://ccdcoe.org/exercises/locked-shields/ .

CHAPITRE III - L'Estonie, fer de lance du soutiens à l'Ukraine

SECTION A - L'Estonie à la tete d'une coalition internationale

L'Estonie joue un rôle particulier dans l'aide à l'Ukraine dans ce contexte de guerre avec la Russie. Elle compte à bien des égards parmi les plus gros soutiens du pays en termes financiers, militaires, humanitaires, ou dans son domaine de prédilection le numérique.

1 - La contribution financière de l'Estonie

Comme nous avons déjà pu l'évoquer au cours de ce développement, l'Estonie est un des pays phares du soutien à l'Ukraine depuis le début du conflit.
Nous pouvons expliquer cela par la solidarité qui unis les Etats post-soviétiques de l'Est de l'Europe, et par les plus de 70 accords bilatéraux qui unissent les deux pays depuis 1993[31].
A ce titre l'Estonie a fait plus que sa part et honore largement ses relations avec l'Ukraine. Nous en parlions en introduction, la république Balte est le pays qui accueille le plus de réfugiés Ukrainiens par rapport à sa population[32]. Selon le *Kiel Institute for the World Economy*, l'aide estonienne pour l'accueil des réfugiés représente une somme équivalente à 1% de son PIB[33].

[31] Kitsoft, Embassy of Ukraine in the Republic of Estonia - Bilateral agreements of Ukraine and Estonia, https://estonia.mfa.gov.ua/en/partnership/105-dogovirno-pravova-baza-mizh-ukrajinoju-ta-jestonijeju .
[32] Ukrainian refugees by country 2023, https://www.statista.com/statistics/1312584/ukrainian-refugees-by-country/
[33] Ukraine Support Tracker - A Database of Military, Financial and Humanitarian Aid to Ukraine, https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/?cookieLevel=not-set .

Les sources concernant les montants d'aide à l'Ukraine sont extrêmement nombreuses et beaucoup de chiffres ne concordent pas notamment à cause des méthodes de calculs incluant ou non les aides aux réfugiés, les aides militaires, ou dans le cas de l'Estonie l'aide bilatérale ou l'aide au sein de l'UE. De plus, la grande majorité des chiffres les plus récents s'arrêtent au 24 février 2023. Plusieurs raisons expliquent cette date, notamment car il est plus facile de compter par tranches de 6 mois ou sur une année à partir du début de la guerre. Cependant selon les chiffre du 13 mai 2023 du site *Visit Ukraine Today*[34] qui dépend du ministère Ukrainien des affaires étrangères, l'Estonie est le pays de l'Union Européenne à l'origine de la plus grande part des financements[35]. Il n'est cependant pas précisé si le chiffre est rapporté à l'équivalent du PIB, mais nous pouvons sans trop de risque affirmer que c'est le cas.

La notion d'échelle est très importante pour prendre pleinement mesure de l'aide estonienne. En effet au niveau européen l'Estonie est le 41ème pays en termes de population[36], et le 34ème PIB[37], le plus bas des 3 pays Baltes dans ces deux catégories.

Enfin pour conclure sur l'aide militaire, nous n'énumérerons pas tout le matériel fournis par le pays, mais soulignerons l'aide de l'Estonie pour former les forces spéciales Ukrainiennes depuis 2015[38], le programme d'aide au rétablissement des blessés de guerres ukrainiens depuis 2016[39], la formations des soldats ukrainiens sur le canon Howitzer[40], la formation des militaires ukrainiens dans l'Opération Interflex[41] ainsi que pour la Mission d'assistance militaire de l'Union européenne en soutien à l'Ukraine[42].

---

[34] Visit Ukraine - RULES OF SAFE VISIT TO UKRAINE, https://visitukraine.today/ .
[35] Military assistance to Ukraine: which countries provide support publicly and which hide arms supplies, https://visitukraine.today/blog/1840/military-assistance-to-ukraine-which-countries-provide-support-publicly-and-which-hide-arms-supplies .
[36] Accueil | Office statistique, https://www.stat.ee/et
[37]Fonds Monétaire International -- Page d'accueil du FMI, https://www.imf.org/fr/Home .
[38] Members of Estonian special forces to help train Ukrainian military, https://news.postimees.ee/3363849/members-of-estonian-special-forces-to-help-train-ukrainian-military , 15 octobre 2015
[39] ERR, *Wounded Ukrainian soldiers to receive treatment in Estonia*, https://news.err.ee/118070/wounded-ukrainian-soldiers-to-receive-treatment-in-estonia , 29 avril 2016.
[40] ERR Anton Aleksejev Kristjan Svirgsten |, ERR in Ukraine: How are Ukrainian soldiers trained in Estonia doing?, https://news.err.ee/1608918101/err-in-ukraine-how-are-ukrainian-soldiers-trained-in-estonia-doing , 17 mars 2023.
[41] ERR ERR News |, Estonia sends more weapons to Ukraine, supports UK training program, https://news.err.ee/1608689164/estonia-sends-more-weapons-to-ukraine-supports-uk-training-program , 18 août 2022.
[42] Pevkur at the meeting of EU defence ministers: Estonia to train Ukrainian soldiers as part of the EU Military Assistance Mission | Kaitseministeerium, https://www.kaitseministeerium.ee/en/news/pevkur-meeting-eu-defence-ministers-estonia-train-ukrainian-soldiers-part-eu-military .

2 - Les programmes européen de soutiens pour la cybersécurité en Ukraine

Forte de son expérience en matière de cybersécurité et de ses infrastructures développées, l'Estonie a logiquement été désignée comme leader pour les projets visant à développer la cybersécurité et la numérisation des services gouvernementaux en Ukraine.

Depuis 2016, l'Union Européenne a mené à bien ou lancé un total de 4 projets différents au profit de la digitalisation de l'Ukraine représentant un investissement de 51 millions d'euros. se sont succédés les projets EGOV4UKRAINE[43], EU4DigitalUA[44] et *EU Support to Strengthening cybersecurity in Ukraine*[45] à partir des succès desquels a été lancé le dernier en date *Digital transformation for Ukraine*[46]. Les deux derniers projets se démarquent des deux autres dans un contexte de guerre encore jamais vu même si les combats touchent le pays depuis 2014. La cybersécurité et la numérisation des services publics pour garantir leur accès à tous les citoyens sont une priorité pour l'Ukraine et ses alliés.

A ce titre l'eGA a été choisi pour mener ces projets. Cette organisation à but non lucratif créée en 2002 par le gouvernement estonien coopère avec des Etats, des entreprises, des organisations internationales, et des experts du monde entier pour promouvoir la gouvernance électronique. L'eGA fait figure d'autorité dans ce secteur car elle collabore avec le gouvernement ukrainien depuis 2011 et mène actuellement 4 projets en collaboration avec le pays[47].

SECTION B - La cyber coopération entre l'Estonie et l'Ukraine

[43] EGOV4Ukraine, https://eufordigital.eu/discover-eu/egov4ukraine/
[44] EU4DigitalUA, https://eufordigital.eu/discover-eu/eu4digitalua/
[45] EU supports cybersecurity in Ukraine with over 10 million euro | EEAS, https://www.eeas.europa.eu/delegations/ukraine/eu-supports-cybersecurity-ukraine-over-10-million-euro_en?s=232&etrans=fr .
[46] euser, EU starts €17.4 million DT4UA project to support Ukraine's digital transformation, https://eufordigital.eu/eu-starts-e17-4-million-dt4ua-project-to-support-ukraines-digital-transformation/ , 3 mars 2023.
[47] Orav Maris, EGA to support Ukraine's digital transformation with € 17,4 M, https://e-estonia.com/ega-to-support-ukraines-digital-transformation-with-e-174-m/ , 21 février 2023.

La coopération entre l'Estonie et l'Ukraine dans le domaine du numérique est un processus continue qui commence véritablement en 2007 lorsque l'Ukraine offre un soutien technique et politique à l'Estonie alors durement impactés par les cyberattaques russes. L'année suivante en 2008 les deux pays signent un accord de coopération pour la cybersécurité, jetant les bases d'une étroite relation. Entre 2008 et aujourd'hui les deux pays participeront et organiseront conjointement plusieurs exercices internationaux, et signeront de nouveaux accords comme celui de 2015 visant à approfondir cette cyber collaboration. A présent dans un contexte de crise pour Kyiv l'Estonie répond présente et fournit à l'Ukraine toute l'aide technique nécessaire à sa cybersécurité et au maintien de ses services gouvernementaux.

1 - Le *Memorandum of Understanding in the field of Digital Transformation*

Le *Memorandum of Understanding in the field of Digital Transformation* entre l'Estonie et l'Ukraine a été ratifié en 2017. Cet accord a été signé le 18 mai 2017 à Tallinn lors d'une visite officielle du Président ukrainien Petro Porochenko. Il marque une étape importante dans la coopération bilatérale entre l'Ukraine et l'Estonie dans le domaine de la transformation numérique et de l'e-gouvernement.

Le MoU établit un cadre de coopération où les deux pays s'engagent à échanger des connaissances, des bonnes pratiques et des expertises dans le domaine de la transformation numérique. Cela inclut des domaines tels que la gouvernance électronique, les services en ligne, la cybersécurité, l'innovation technologique, l'e-gouvernement, l'éducation numérique, et d'autres aspects liés à la numérisation des sociétés dans lesquels l'Estonie est particulièrement compétente.

L'objectif principal de cet accord est de créer un environnement favorable à la croissance et à l'innovation dans le secteur numérique, en favorisant l'échange d'expériences et de connaissances entre l'Estonie et l'Ukraine.

L'accord reflète l'engagement des deux pays à tirer parti des avantages de la transformation numérique pour stimuler le développement économique, améliorer les services publics, renforcer la compétitivité et la résilience dans les contexte de crise comme celui que traverse l'Ukraine et qu'a connu l'Estonie à travers les cyberattaques russes à travers l'utilisation des technologies de l'information et de la communication.

Le MoU a été mis à jour à plusieurs reprises[48] et les termes ont donc évolué avec le temps en fonction des besoins et des circonstances, notamment l'invasion russe du 24 février 2022. Cependant seule la version originale du texte est trouvable en ligne sur le site du ministère estonien de l'économie et de la communication[49].

2 - L'Estonie dans le développement de Diia

L'un des projets phares de la collaboration Estonie-Ukraine a été la mise en place de l'application Diia[50] en Ukraine qui vise à offrir aux citoyens et aux entreprises un accès simplifié aux services publics et à augmenter l'efficacité de l'administration.

L'Estonie a joué un rôle important dans le développement du projet Diia en partageant son expertise en gouvernance électronique. En tant que leader reconnu dans ce domaine, l'Estonie a apporté son soutien technique et son savoir-faire pour aider l'Ukraine à mettre en place ce portail gouvernemental ergonomique et efficace.

L'eGA, dont nous avons parlé précédemment, est l'une des organisations estoniennes les plus actives dans la coopération avec l'Ukraine pour la mise en œuvre de l'application. Elle a fourni des formations, des conseils et des services d'assistance technique au sein de ses locaux pour aider l'Ukraine à développer les fonctionnalités et les processus nécessaires à la réussite du projet.

L'expérience estonienne en matière de gouvernance électronique, notamment avec le système d'identification électronique et le portail gouvernemental estonien eesti.ee[51], a été partagée avec l'Ukraine pour guider la conception et la mise en œuvre de Diia. L'Estonie a également aidé à renforcer la sécurité des données et à mettre en place des mesures de protection de la vie privée pour assurer la confiance des utilisateurs et la sécurisation de leur données.

---

[48] Memorandum of cooperation in the field of digital transformation was signed in presence of the Presidents of Ukraine and Estonia, https://www.president.gov.ua/en/news/u-prisutnosti-prezidentiv-ukrayini-ta-estoniyi-pidpisano-mem-58585 .

[49] https://mkm.ee/media/8212/download

[50] Державні послуги онлайн | Дія, https://diia.gov.ua/ .

[51] *Estonie.ee*, https://www.eesti.ee/et .

Pour l'Estonie l'Ukraine est depuis 2014 et encore plus depuis 2022 une sorte de grand laboratoire qui permet aux Estoniens d'éprouver les réponses opérationnelles cyber à une attaque russe. L'utilisation massive des smartphones pour assurer la continuité du service public ukrainien malgré la crise a été le moteur d'un développement conjoint et rapide de Diia, première solution mobile de gestion de l'identité.

De plus, devant le succès de l'application et de l'avantage concret qu'elle confère au gouvernement, l'Estonie à décider de développer mRiik[52] sa propre application gouvernementale basée sur Dii.

[52] Orav Maris, Estonia to pilot a national mobile app based on the Ukrainian Diia application, https://e-estonia.com/estonia-to-pilot-a-national-mobile-app-based-on-the-ukrainian-diia-application/ , 2 septembre 2022.

Conclusion :

Comment l'Estonie, petite nation Balte de 1.3 millions d'habitants, s'est construite comme puissance incontournable du monde cyber et quelle est son activité dans le conflit entre la Russie et l'Ukraine aux côtés de cette dernière et de ses alliés occidentaux?

Pour conclure ce travail et répondre à la question nous pouvons retenir les trois points essentiels qui suivent. Premièrement, nous pouvons désigner la Russie comme responsable de la construction de l'Estonie comme cybernation. En effet, c'est d'une certaine manière l'URSS qui a permis à l'Estonie de lancer son grand pari sur le numérique, et c'est la Russie qui à travers les cyberattaques de 2007 et de toutes celles qui ont succédés, a permis au pays de s'aguerrir, de se développer et de s'affirmer comme cyberpuissance.

Deuxièmement, sa situation géographique, même si dans l'univers cyber les distances et les frontières correspondent à une autre réalité que celle que nous connaissons, l'Estonie constitue un avant post stratégique aux frontières de la Russie. Par ailleurs, son expérience et ses compétences en matière de cybersécurité, ainsi que ses investissements dans le domaine au niveau de la formation, des infrastructures et des politiques gouvernementales en font le cheval de bataille de l'OTAN et un lieu privilégié pour échanger et former les alliés de l'organisation ou de l'union européenne.

Enfin, porté par un passé commun avec l'Ukraine, et animé de la même solidarité qui unit tous les États post-soviétiques et post-communistes de l'Est de l'Europe, l'Estonie est un pays clé du soutiens à l'Ukraine et surtout extrêmement actif tant au niveau humanitaire, économique et militaire surtout dans la cyberdéfense, sans oublier l'aide direct au gouvernement de Kiev pour le maintien des services gouvernementaux et le développement de solutions agiles dans un pays ravagé par la guerre.

Ce travail trouve ses limites tout d'abord dans la dimension temporelle. En effet le conflit étant encore en cours, le manque de recul, de sources officielles et de travaux universitaires sur l'implication estonienne dans la cyberguerre qui se joue viennent complexifier les recherches. A ce sujet, le thème en lui-même présentant une dimension sensible, il est logique que des informations détaillées soient complexes à mettre sur la table. Ainsi le manque de détails et de sources pour certains passages peuvent nuire à la qualité du travail.
Enfin, comme annoncé dans le prologue, ce mémoire de stage s'apparente plus à une cour mémoire de recherche sur une thématique en lien avec le stage, qu'un rapport de stage problématisé.

Pour ouvrir le débat nous pouvons nous inspirer des exemples estoniens et ukrainiens et nous questionner sur la manière d'établir en France un modèle d'e-gouvernance aussi performant, fiable et pratique que celui de la nation Balte.

Bibliographie :

Sources universitaires

- Chalvin Antoine, « L'ombre du soldat de bronze », in Le Courrier des pays de l'Est, no 4, vol. 1062, 2007, p. 6-16.

Textes officiels / lois

- Principles of Estonian Information Policy, https://ega.ee/publication/principles-of-estonian-information-policy/.
-https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy/@@download_version/9933548 31bfc4d689c20492459f8a086/file_en
- NATO, Warsaw Summit Communiqué issued by NATO Heads of State and Government (2016), https://www.nato.int/cps/en/natohq/official_texts_133169.htm .
-https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
- NATO PA, https://www.nato-pa.int/document/2022-offence-defence-natos-cyber-challenge-report-pinotti-015-dscfc , 23 juin 2023.
- https://mkm.ee/media/8212/download

Articles

- Russian minority in Estonia turns its back on Putin, https://www.euractiv.com/section/politics/short_news/russian-minority-in-estonia-turns-its-back-on-putin/ , 23 mars 2022.
- Soldat de bronze: la Russie soulèvera la question sur la situation en Estonie au Conseil de l'Europe | International | RIA Novosti, https://archive.wikiwix.com/cache/index2.php?url=http%3A%2F%2Ffr.rian.ru%2Ftrend%2Fdemontage_talinn%2F#federation=archive.wikiwix.com&tab=url.

- Gaskell Adi, How Estonia Became The Digital Leader Of Europe, https://www.forbes.com/sites/adigaskell/2017/06/23/how-estonia-became-the-digital-leaders-of-europe/.
- Européennes : comment la petite Estonie est devenue le royaume du tout-numérique et de l'e-administration, https://www.tf1info.fr/high-tech/elections-europeennes-2019-comment-l-estonie-est-devenue-le-royaume-du-tout-numerique-et-de-l-e-administration-2122042.html , 24 mai 2019.
- *How it all began? From Tiger Leap to digital society*, https://www.educationestonia.org/tiger-leap/.
- L'Estonie, pays pilote de l'Internet, https://www.latribune.fr/archives/2004/entreprises/communication/id7aa7bbacce3b8e05c1256e860045a9e4/lestonie-pays-pilote-de-linternet.html , 19 octobre 2008.
- Authoritatively, Who Was Behind The Estonian Attacks? - Hacked Off - Dark Reading, https://web.archive.org/web/20090701212951/http://www.darkreading.com/blog/archives/2009/03/authoritatively.html , 1 juillet 2009.
- CCDCOE, https://ccdcoe.org/library/publications/estonia-after-the-2007-cyber-attacks-legal-strategic-and-organisational-changes-in-cyber-security/ .
- NATO, Cyberdéfense, https://www.nato.int/cps/fr/natohq/topics_78170.htm .
- NATO, 2022 NATO Summit, https://www.nato.int/cps/en/natohq/news_196144.htm .
- Italy U. S. Mission, NATO's 2022 Cyber Defense Pledge Conference, https://it.usembassy.gov/natos-2022-cyber-defense-pledge-conference/ , 9 novembre 2022.
- Exercise Cyber Coalition 2022, https://shape.nato.int/news-releases/exercise-cyber-coalition-2022-.aspx .
- Le COMCYBER participe à CYBER COALITION 2022, exercice international de grande envergure de l'OTAN | Ministère des Armées, https://www.defense.gouv.fr/ema/actualites/comcyber-participe-cyber-coalition-2022-exercice-international-grande-envergure-lotan , 9 décembre 2022.
- Locked Shields, https://ccdcoe.org/exercises/locked-shields/ .

- Military assistance to Ukraine: which countries provide support publicly and which hide arms supplies, https://visitukraine.today/blog/1840/military-assistance-to-ukraine-which-countries-provide-support-publicly-and-which-hide-arms-supplies .
- Pevkur at the meeting of EU defence ministers: Estonia to train Ukrainian soldiers as part of the EU Military Assistance Mission | Kaitseministeerium, https://www.kaitseministeerium.ee/en/news/pevkur-meeting-eu-defence-ministers-estonia-train-ukrainian-soldiers-part-eu-military .
- ERR Anton Aleksejev Kristjan Svirgsten |, ERR in Ukraine: How are Ukrainian soldiers trained in Estonia doing?, https://news.err.ee/1608918101/err-in-ukraine-how-are-ukrainian-soldiers-trained-in-estonia-doing , 17 mars 2023.
- ERR ERR News |, Estonia sends more weapons to Ukraine, supports UK training program, https://news.err.ee/1608689164/estonia-sends-more-weapons-to-ukraine-supports-uk-training-program , 18 août 2022.
- ERR, *Wounded Ukrainian soldiers to receive treatment in Estonia*, https://news.err.ee/118070/wounded-ukrainian-soldiers-to-receive-treatment-in-estonia , 29 avril 2016
- Members of Estonian special forces to help train Ukrainian military, https://news.postimees.ee/3363849/members-of-estonian-special-forces-to-help-train-ukrainian-military , 15 octobre 2015.
- Orav Maris, EGA to support Ukraine's digital transformation with € 17,4 M, https://e-estonia.com/ega-to-support-ukraines-digital-transformation-with-e-174-m/ , 21 février 2023.
- EU supports cybersecurity in Ukraine with over 10 million euro | EEAS, https://www.eeas.europa.eu/delegations/ukraine/eu-supports-cybersecurity-ukraine-over-10-million-euro_en?s=232&etrans=fr .
- euser, EU starts €17.4 million DT4UA project to support Ukraine's digital transformation, https://eufordigital.eu/eu-starts-e17-4-million-dt4ua-project-to-support-ukraines-digital-transformation/ , 3 mars 2023.
- EU4DigitalUA, https://eufordigital.eu/discover-eu/eu4digitalua/ .

- EGOV4Ukraine, https://eufordigital.eu/discover-eu/egov4ukraine/
- Memorandum of cooperation in the field of digital transformation was signed in presence of the Presidents of Ukraine and Estonia, https://www.president.gov.ua/en/news/u-prisutnosti-prezidentiv-ukrayini-ta-estoniyi-pidpisano-mem-58585 .
- Orav Maris, Estonia to pilot a national mobile app based on the Ukrainian Diia application, https://e-estonia.com/estonia-to-pilot-a-national-mobile-app-based-on-the-ukrainian-diia-application/ , 2 septembre 2022.

Pages Web

- ERR, News, https://news.err.ee/
- Ukrainian refugees by country 2023, https://www.statista.com/statistics/1312584/ukrainian-refugees-by-country/
- Story, https://e-estonia.com/story/.
- Tiigrihüpe, https://kompass.harno.ee/tiigrihupe/.
- EATA | Missions and operations, https://www.eata.ee/en/nato/missions-and-operations/ .
- Kaspersky Transparency Center | Kaspersky, https://www.kaspersky.com/capacity-building .
- Exercises, https://ccdcoe.org/exercises/ .
- Kitsoft, Embassy of Ukraine in the Republic of Estonia - Bilateral agreements of Ukraine and Estonia, https://estonia.mfa.gov.ua/en/partnership/105-dogovirno-pravova-baza-mizh-ukrajinoju-ta-jestonijeju .
- Ukraine Support Tracker - A Database of Military, Financial and Humanitarian Aid to Ukraine, https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/?cookieLevel=not-set .
- Visit Ukraine - RULES OF SAFE VISIT TO UKRAINE, https://visitukraine.today/ .
- Fonds Monétaire International -- Page d'accueil du FMI, https://www.imf.org/fr/Home .

- Accueil | Office statistique, https://www.stat.ee/et
- Estonie.ee, https://www.eesti.ee/et .
- Державні послуги онлайн | Дія, https://diia.gov.ua/ .

Vidéos

- Arts & Métiers Alumni, E-gouvernement et menace cyber : le cas de l'Estonie, s.l., s.n., 2018.
- NATO MILITARY SHAPE, Cyber Coalition 2022, NATO's flagship cyber defence exercise, s.l., s.n., 2022.