C'est vrai que le fait notamment de ces attentats contre les personnes présentes lors de cette de ce festival avec une population jeune équipée de téléphones portables et qui donc ainsi à alimenter des réseaux sociaux en images, en sons, et ça c'est quelque chose qui fait partie de cet affrontement informationnel.
Bonjour Nicolas Rpagian.
Bonjour.
Vous êtes spécialiste de la cyber sécurité et de la cyber guerre auteur de plusieurs livres sur le sujet.
Le dernier s'intitule Frontière au pluriel.com.
Vous êtes également vice-président du cabinet Headminds Partners.
Vous vous trouvez actuellement d'ailleurs aux assistes de la cyber sécurité à Monaco.
Et j'imagine qu'on doit parler notamment de ce qui vient de se passer en Israël parce qu'il y a ce que l'on voit, les images, mais il y a forcément, et on le sait, un volet cyber à tout ça, il y a cette guerre qui est ancienne entre Israël et le ramasse.
Alors c'est certain que si on compare avec le récent conflit et l'entrée en guerre en Ukraine, on n'a pas documenté, on n'a pas constaté d'attaque ayant visé les infrastructures institutionnelles, économiques, administratives, voire militaires israéliens.
Donc ça ce n'est pas un sujet à part entière, ce n'est pas un élément conséquent.
Par contre, ce qui est certain, c'est qu'on a documenté par le passé des intrusions notamment pour viser à collecter du renseignement.
Et c'est vrai qu'il avait été établi que aussi bien des comptes, des profils sur des réseaux sociaux et aussi grand public que Facebook, mais également sous prétexte de faire des applications, au tout cas des sites de rencontre, de manière à entrer en contact avec des conscris afin de collecter des informations quant au positionnement de leurs unités et à des projections et à des activités qui pouvaient ainsi renseigner sur la localisation de troupes et éventuellement des positionnements qui seraient utiles en cas de conception de plans et d'attaques terrestres et d'attaques totalement physiques.
Alors évidemment, dans un environnement aussi violent que ce qui est passé ces dernières heures, la dimension cyber peut paraître accessoire parce qu'il y a un véritable engagement de la vie humaine dans ses théâtres d'opération.
Par contre, ce qui est certain, c'est qu'on a le deuxième volet qui a été totalement en tout cas pris en compte, qui est le volet informationnel.
Et c'est vrai que le fait notamment de ces attentats contre les personnes présentes lors de ce festival, de cet événement festif avec une population jeune, équipée de téléphones portables et qui donc ainsi a alimenté des réseaux sociaux en images, en sons de manière extrêmement large.
Et ça, c'est quelque chose qui fait partie de cet affrontement informationnel.
Il est toujours délicat de parler de guerre en comparaison avec l'engagement de la vie de femmes et d'hommes évidemment, mais en tout cas d'un affrontement informationnel qui utilise le numérique pour venir amplifier le sentiment de erreur, le sentiment d'inquiétude et donc ainsi essayer d'élargir la cible de ce conflit qui est au début géographiquement localisé.
Là, vous évoquez toutes les vidéos qui circulent, certaines qui sont vraiment instrumentalisées pour être de la propagande et puis d'autres qui ne sont que des témoignages

de personnes, mais qui ne sont pas neutres non plus parce qu'elles influent dans un sens ou dans un autre.
Nicolas Repagiant, il faut dire un mot, s'il y a quand même les tensions préexistantes entre Israël, ce groupe palestinien, l'Iran également, tout cela, il y a aussi un volet cyber et cyberguerre depuis des années en fait.
Alors, c'était un outil soit pour capter du renseignement, essayer justement de comprendre qu'elles étaient les stratégies, les plans et ça, c'est quelque chose qui va s'organiser à babouille, faire en sorte au contraire de créer le moins de perturbation possible chez son adversaire, de manière précisément à ce qu'il ignore la captation de données, le fait qu'on va ainsi compiler du renseignement.
La particularité, c'est que ça peut se faire tout azimuth puisque à ce moment-là, si ça doit venir en préparation d'une agression physique qui va être planifiée, effectivement, il y a le temps de la préparation, de la compilation de ces données pour essayer précisément de comprendre quels sont les positionnements des troupes, quels sont même l'état d'esprit des personnes que l'on va avoir en face et ça, c'est important à considérer.
Ce qui est certain, c'est qu'aujourd'hui, on voit les limites dans un monde totalement, je l'ai dit, physique de la dimension cyber, puisque précisément, ce sont des femmes, des hommes, des attaques de manière très rustique, en quelque sorte, qui vont venir empiéter sur un territoire et le numérique va être utilisé à des fins d'accélération de la crise, d'amplification de la crise, précisément pour essayer de la porter au-delà de ces frontières physiques et c'est pour ça que c'est une question et on voit d'ailleurs les messages qui ont été adressés à X, l'anciennement Twitter, notamment par la Commission européenne, mais pas seulement pour réagir, pour faire en sorte de dire, voilà, votre obligation de modération des contenus, de contrôle en tout cas d'un certain type de publication puisque vous l'avez mentionné, on a à la fois des publications sous le coup de l'émotion de gens qui sont présents dans des circonstances très particulières et qui vont publier ces informations et puis effectivement une part de désinformation pour soit utiliser des images qui ont été tournées dans d'autres contextes, soit pour biaiser telle ou telle circonstance avec un éclairage très spécifique et politiquement biaisé.
Et donc c'est la raison pour laquelle justement la Commission européenne a une fois de plus rappelé à les grandes plateformes, essentiellement X parce que c'est un théâtre particulièrement apprécié des opérations de manipulation informationales pour précisément repérer, suspendre et le cas échéant, fermer des comptes qui manifestement auraient une activité délibérément frauduleuse du point de vue de la rigueur de l'information.
Il y a autre chose qui frappe, c'est qu'Israël est connu pour être un pays très en avance en matière de technologie notamment de surveillance électronique et on a l'impression notamment que dans cette opération du 7 octobre, une impression de surprise comme on avait eu pour l'Ordion septembre, est-ce que c'est une nouvelle marque de la défaillance du renseignement 100% ou en tout cas très électronique et numérique ?
En tout cas parce qu'il faut considérer qu'il y a vraisemblablement un soutien étatique et que ce n'est pas uniquement la communauté palestinienne mais que des moyens de services de renseignement
de rends étatiques ont été à la manœuvre pour concevoir, préparer et opérationnaliser les actions

en question, ça c'est la première chose. La deuxième c'est évidemment il y aura de toute façon toujours un avantage stratégique de la part de l'attaquant qui lui va choisir son mode opératoire, sa cible et les terrains d'action de ces opérations d'attaque ou de déstabilisation. Donc ça c'est un prix rookie ou en tout cas un avantage qui est offert à l'assaillant. Troisième chose c'est il faut garder à l'esprit la notion d'asémitrie et de rusticité. Lorsqu'il s'agit de mettre à mal le dome d'acier, il est évident que les missiles qui vont être utilisés par Israël pour neutraliser ce qui arrive sur son territoire vont être des missiles beaucoup plus coûteux que éventuellement les charges qui vont être conçues pour précisément tenter de laisser évidemment de tuer sur place et donc on voit que les moyens qui s'affrontent sont forcément asymétriques en termes de coûts et donc en termes de moyens techniquement consacrés à cela. Quatrième point c'est évidemment le fait de pouvoir l'aurer des systèmes, aveugler des systèmes de sécurité. On l'a vu sur des postes frontières qui manifestement il y avait peut-être une trop grande confiance dans la capacité technique de supervision. C'est vrai que de la même manière que ces ailes volantes qui ont été utilisées, bon bah pour un certain nombre d'outillages technologiques, quelquefois on les assimile à des oiseaux, à éventuellement à des perturbations naturelles et donc effectivement dès lors que vous êtes en dessous des lignes de radar, vous ne suscitez pas les systèmes d'alerte et donc ce n'est que tardivement ou de manière imprécise que l'on va pouvoir caractériser la nature de la molasse et donc entreprendre une réponse et une riposte et c'est la raison pour laquelle effectivement une fois qu'un dispositif de sécurité est mis en oeuvre l'assaillant va faire en sorte de proportionner ces outils d'attaque de manière à essayer de passer outre justement et de retarder le déclenchement des systèmes de sécurité. C'est pour ça que c'est une, en tout cas ça plaît d'une fois de plus pour une combinaison technique et humaine et de ne pas avoir de confiance mais de délégation exclusive à la technologie puisque l'esprit humain va faire en sorte précisément de trouver le moyen de l'aurer, c'est vraiment le terme, l'aurer les dispositifs de détection. En plus ces systèmes de détection automatique dont vous parlez ont été neutralisés en fait dès le départ par des bombardements, par des drones etc. En fait le principe c'est de faire en sorte que si on fait une analogie triviale évidemment on regarde les circonstances mais c'est un peu la caméra, si il n'y a pas dans votre maison, votre appartement, la caméra peut détecter des éléments mais s'il n'y a pas de vigile capable d'intervenir rapidement avec diligence, avec des moyens adaptés à la nature de notre région, effectivement ça relativise l'utilité, la performance du dispositif. Donc là c'est les vrais choix stratégiques mais qui, et même au-delà du caractère tragique des circonstances précises, plaident précisément pour une combinaison des éléments de sécurité physique, des éléments techniques et également des éléments humains. Et ça c'est certainement pour ceux qui ont vocation à protéger les équipements, les infrastructures, une illustration supplémentaire de l'importance de cette combinaison et de ne pas surfavoriser notamment la seule dimension technique qui forcément doit apprendre dès lors qu'elle aurait été l'auré et détecte un moyen de contournement dès lors qu'on lui a enseigné et donc évidemment la créativité humaine est lui est beaucoup plus favorable et va être à même de l'auré et de tromper le dispositif technique de détection. Merci beaucoup Nicolas Pagian, spécialiste de la cyber sécurité et de la cyber guerre.