De qui se cache-t-on ? Modélisation des menaces et risque 'relationnel'

Ksenia Ermoshina, Francesca Musiani

Ce texte est la version auteur de Ksenia Ermoshina, Francesca Musiani, 2024, « De qui se cache-t-on ? Modélisation des menaces et risque 'relationnel' », pp. 171-192 in Christine Petr et Olivier Segard (eds.) *Le droit à la vie privée. L'urgence de l'hygiène numérique*, Rennes, Presses Universitaires de Rennes. Présentation de l'ouvrage

De qui se cache-t-on ? Modélisation des menaces et risque « relationnel »

Ksenia Ermoshina et Francesca Musiani

Afin de dissimuler, de brouiller et de masquer les communications privées et autres activités en ligne, il existe maintenant dans le domaine de la messagerie chiffrée un vaste éventail de solutions, dont chacune est conçue pour protéger ses usagers vis-à-vis « d'adversaires » bien précis. Les fonctions de sécurité et de confidentialité intégrées aux différents protocoles proposent divers degrés de protection et permettent aux utilisateurs de dissimuler différentes parties de leur identité en ligne. Ce chapitre aborde la manière dont sont déployés, dans le développement de systèmes de messagerie chiffrée, des instruments comme la « modélisation des menaces » et l'analyse des risques, servant à identifier ce dont l'utilisateur doit être caché ou à analyser la probabilité qu'une menace se réalise. Il devient important non seulement de savoir de qui l'on cherche à éviter l'attention, mais aussi d'évaluer la probabilité effective que l'on soit amené à « rencontrer » cet adversaire. De fait, les utilisateurs ne se perçoivent pas tant comme porteurs d'une identité unique que comme un ensemble de « profils » ou de « personnages », dont chacun peut nécessiter ses propres modèles de « soin de sa personne » (*self-care*) numérique employant des ensembles d'outils bien précis. Le fait que chacune de ces différentes identités appelle un modèle singulier de comportement en ligne mène à la création d'une sécurité dite « par compartimentation ». Dans ce chapitre, nous explorerons la dimension relationnelle et socialement définie d'un concept de risque qui, en sécurité informatique, dépend fortement des graphes sociaux des utilisateurs et de leurs contextes de communication[1].

[1] Ce travail a été financé par le projet européen NEXTLEAP (European Union's Horizon 2020 Framework Programme for Research and Innovation – H2020-ICT-2015, ICT-10-2015 – grant agreement nº 688722).

Ce chapitre est une traduction par Paco Libbrecht de l'article Ermoshina, K. & F. Musiani, 'Hiding from Whom? Threat Models and In-the-Making Encryption Technologies', *Intermédialités: Histoire et théorie des arts, des lettres et des techniques*, 32 (2019), numéro spécial Cacher/Concealing. Nous l'avons également présenté et commenté au colloque annuel de l'*International Association for Media and Communication Research* qui s'est tenu à Eugene, Oregon, du 7 au 11 juillet 2018. Nous adressons nos sincères remerciements à la Commission Nationale Informatique et Libertés et à l'Inria qui ont sélectionné ce travail comme *runner-up* lors de l'édition 2019 de leur Prix « Protection de la Vie Privée ».

Créer et dissimuler une présence en ligne

Par suite d'une récente augmentation dans la variété des cas d'usage de messageries sécurisées chiffrées, un certain nombre d'outils de protection de la vie privée ont vu le jour, proposant toute une gamme de solutions pour dissimuler les communications privées et autres échanges en ligne. Des solutions centralisées les plus populaires comme Wire, Telegram, Signal et WhatsApp aux plateformes décentralisées moins répandues comme Ricochet ou Briar en passant par les clients mèl prenant en charge le cryptage PGP, toutes ces solutions sont spécifiquement conçues pour se protéger « d'adversaires » bien précis. Les fonctions de sécurité et de confidentialité intégrées aux divers protocoles proposent différents degrés de protection, et permettent aux utilisateurs de « cacher » différentes parties de leur identité en ligne.

La considérable variété de dispositifs de dissimulation développés pour nos outils de communication vient répondre à la complexité croissante du rapport qu'entretiennent les usagers d'Internet avec la circulation de leurs données personnelles en ligne. En effet, nos traces en ligne sont intégrées dans les couches plurielles de l'infrastructure matérielle et logicielle d'internet. Notre identité peut être révélée non seulement par le contenu de nos messages, mais aussi par les identifiants uniques de nos appareils (tels que les adresses Mac), nos adresses IP et d'autres métadonnées connexes, et c'est pourquoi nous assistons à un « tournant vers l'infrastructure » dans la protection de la vie privée et sa gouvernance[2]. Cela soulève notamment les questions de savoir lesquels de nos multiples identifiants en ligne peuvent être considérés comme personnels, quelles données nous avons à cacher, et à qui il faut les cacher, ainsi que – en écho à la « théorie de la mosaïque » de David Pozen[3] – à partir de quand une combinaison de plusieurs informations *a priori* non identifiantes permet-elle suffisamment de personnalisation pour désanonymiser un utilisateur.

A la lumière de travaux antérieurs, tels que l'anthropologie des filtres anti-spam[4], nous concevons les systèmes cryptographiques comme des tamis qui séparent les éléments d'information devant être cachés de ceux qui peuvent être montrés. Les algorithmes de cryptage se présentent comme des inverses, ou des ombres, des informations qu'ils trient. Pour concevoir un outil de protection de la vie privée, il faut imaginer le « pire des mondes possibles », un monde construit à partir de divers scénarios impliquant des risques, des incertitudes et des failles dans les systèmes de sécurité. L'identification d'un modèle de menace permet de convenir du seuil d'anonymat et de confidentialité qui convient à un contexte d'utilisation particulier. Ainsi, différents utilisateurs peuvent définir leur adversaire de différentes manières, sont susceptible d'être en désaccord sur les types de données qui

[2] Francesca Musiani, Derrick L. Cogburn, Laura DeNardis & Nanette S. Levinson (eds.). *The Turn to Infrastructure in Internet Governance*, New York, Palgrave/Macmillan, 2016.

[3] David E. Pozen, "The mosaic theory, national security, and the freedom of information act", *The Yale Law Journal*, vol. 115, n° 3, 2005, pp. 628-679.

[4] Paul Kockelman, "The anthropology of an equation. Sieves, spam filters, agentive algorithms, and ontologies of transformation", *HAU: Journal of Ethnographic Theory*, vol. 3, n° 3, 2013, pp. 33-61.

devraient être dissimulées (ou vont en tout cas avoir à trouver un terrain d'entente), et doivent choisir les outils les plus susceptibles de leur donner le niveau de protection dont ils ont besoin. En fonction des différents cas d'usage, en allant de situations à faible risque où les usagers n'ont « rien à cacher » à des scénarios à haut risque dans des zones de guerre ou sous des gouvernements autoritaires, les utilisateurs, les formateurs et les développeurs co-construisent des modèles de menace et décident des données à dissimuler et des manières de le faire. A cette fin, ils s'appuient parfois sur une gamme d'arts de faire déployés par les utilisateurs pour « détourner »[5] les outils de cryptage existants et développer leurs propres moyens de se cacher.

Afin de comprendre la construction des modèles de menace, il sera utile de retourner sur les travaux interdisciplinaires de la dernière quinzaine d'années ayant exploré la dimension « collective » de la vie privée et la mesure dans laquelle sa protection nécessite des rapports d'interdépendance entre de multiples facteurs et acteurs. Par exemple, Daniel Solove a décrit l'identification progressive des contours de la représentation sociale en ligne par le biais des traces informationnelles que les différentes interactions laissent dispersées dans toutes sortes de réseaux et de bases de données[6]. Ces traces sont au cœur non seulement des tentatives des États et des entreprises de suivre les citoyens et les utilisateurs et d'établir leurs profils, mais aussi des stratégies des militants visant à dénoncer les abus des entreprises et des États. La protection de sa vie privée dans le monde connecté est donc un exercice de gestion des visibilités[7]. Dans le même ordre d'idées, en mettant l'accent sur les manières dont les utilisateurs peuvent agir sur leur propre vie privée, Antonio Casilli a montré comment le droit à la vie privée était devenu une « négociation collective » dont l'objectif principal est de maîtriser sa projection de soi dans les interactions sociales[8]. Paul Dourish et Ken Anderson ont su résumer et distiller le message qu'avance cette approche de la vie privée et de la sécurité en écrivant qu'il s'agit de « concepts difficiles à gérer d'un point de vue technique précisément parce qu'ils sont pris dans des rhétoriques et des pratiques collectives élargies du risque, du danger, du secret, de la confiance, de la moralité, de l'identité, et plus encore », et en soutenant que nous devrions nous diriger « vers une vision holistique de pratiques d'information situées et collectives »[9].

Les études sur la surveillance ont également porté une attention toute particulière aux dimensions collectives et relationnelles de la surveillance, de la vie privée et de la sécurité. Certains auteurs désireux d'explorer le concept de résistance ont souligné la nature algorithmique et « rhizomatique »

---

[5] Michel Callon, "The Sociology of an Actor-Network: The Case of the Electric Vehicle", in Michel Callon, John Law and Arie Rip (eds.), *Mapping the Dynamics of Science and Technology: Sociology of Science in the Real World*, London, Macmillan Press, 1986, pp. 19-34.

[6] Daniel J. Solove, "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, vol. 154, n°3, 2006, pp. 477-560.

[7] Mikkel Flyverbom, Paul M. Leonardi, Cynthia Stohl, Michael Stohl, "The Management of Visibilities in the Digital Age", *International Journal of Communication*, n°10, 2016, pp. 98-109.

[8] Antonio Casilli, « Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée », in *Rapport du Conseil d'Etat*, 2015, pp. 423-434.

[9] Paul Dourish and Ken Anderson, "Collective information practice: exploring privacy and security as social and cultural phenomena", *Human-computer interaction*, vol. 21, n°3, 2006, pp. 319-342.

des nouvelles pratiques de surveillance et les réponses nécessaires pour les contrer[10] ; d'autres ont expliqué qu'une conceptualisation traditionnelle de la surveillance, impliquant une relation exclusive entre le surveillant et son objet, ne prenait pas correctement en compte les « assemblages surveillants » (y compris ceux qui cherchent à répondre à la surveillance) que l'on observe actuellement dans les médias en réseau, et qui transforment les cibles et les hiérarchies des activités de surveillance tout en reconfigurant au passage la notion de vie privée[11].

Bien qu'étant fondées sur des recherches qui démontrent l'omniprésence de la surveillance numérique et font écho à la conceptualisation de la surveillance en tant qu' « assemblage », certaines des contributions aux études de la surveillance en ligne et de la protection de la vie privée visent explicitement à fournir des « guides » pratiques aux utilisateurs. C'est notamment le cas du livre de Finn Brunton et Helen Nissenbaum *Obfuscation*, qui vise à la fois à présenter un raisonnement et à fournir un ensemble d'outils destinés à « produire délibérément des informations ambigües, désordonnées et fallacieuses et à les ajouter aux données existantes afin de perturber la surveillance et la collecte des données personnelles », ce qui inclut notamment des stratégies de sabotage et de refus d'obtempérer[12]. Quoi qu'il se focalise plus sur le contexte canadien, le travail de Lex Gill et de ses collègues vise également à fournir un « guide de terrain » des débats sur le chiffrement et à présenter des suggestions pratiques pour « les décideurs politiques, les professionnels du droit, les universitaires, les journalistes et les militants qui tentent de s'orienter parmi les effets et répercussions complexes de cette technologie »[13]. Il est intéressant de prendre acte de la fréquence croissante de ce type de contributions – les guides pratiques publiés par des universitaires spécialistes du domaine. Ces textes créent des hybrides situés quelque part entre contributions universitaires et outils pratiques destinés à accompagner la prolifération des outils et de leurs éventuels cas d'usage. Ainsi, de tels textes contribuent à co-déterminer concrètement les réponses des utilisateurs à la surveillance et les actions de protection de la vie privée en ligne.

---

[10] Aaron Martin, Rosamunde van Brakel and Daniel Bernhard, "Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework", *Surveillance & Society*, vol. 6, n°3, 2009, pp. 213-232.

[11] Kevin D. Haggerty and Richard D. Ericson, "The Surveillant Assemblage", *British Journal of Sociology*, vol. 51, n°4, 2000, pp. 605-622.

[12] Finn Brunton, Helen Nissenbaum, *Obfuscation: A user's guide for privacy and protest*. Cambridge, MA: The MIT Press, 2015.

[13] Lex Gill, Tamir Israel, Christopher Parsons, " Shining a Light on the Encryption Debate: A Canadian Field Guide", report by Citizen Lab and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, 2018, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf

« Connaître son ennemi » : la modélisation de menace comme outil de formation

En ingénierie du logiciel et dans les études de conception, la modélisation de menace est considérée comme partie intégrante d'un cycle de conception normal, où les « besoins de sécurité » sont conçus comme l'une des multiples facettes d'un processus de conception complexe : « Nous devons tenir compte des besoins en matière de sécurité tout au long du processus de conception, tout comme nous le faisons pour les performances, la convivialité, la localisabilité, la facilité d'entretien ou toute autre facette du produit »[14]. Appliquée au processus de développement logiciel, la modélisation des menaces est définie comme un « processus formel d'identification, de documentation et d'atténuation des menaces pour la sécurité d'un système logiciel »[15]. La modélisation des menaces permet aux équipes de développement d'examiner l'application « au travers du regard d'un adversaire potentiel » afin d'identifier les principaux risques pesant sur sa sécurité. Cependant, les processus et techniques de modélisation des menaces sont également appliqués aux agents humains, afin de déceler des vulnérabilités dans les modèles de comportement des utilisateurs (aussi bien en ligne qu'hors ligne), d'identifier les informations sensibles « à protéger », de définir les potentiels adversaires, d'évaluer leurs capacités et de proposer des solutions de protection et d'atténuation des risques.

L'idée de modéliser la menace au niveau des utilisateurs plutôt que des systèmes d'information vient du fait qu'il est difficile, si ce n'est impossible, de « se cacher de tout le monde ». Comme le dit l'Electronic Frontier Foundation (EFF), une ONG de premier plan dans le domaine de la sécurité numérique :

Il est impossible de se prémunir contre toutes les sortes de ruses ou d'assaillants. Vous devriez donc déterminer en priorité qui pourraient vouloir vos données, ce qu'ils pourraient en tirer et la façon dont ils pourraient se les procurer. On appelle modélisation des menaces la détermination d'un ensemble d'attaques possibles contre lesquelles vous souhaitez vous prémunir[16].

La modélisation des menaces va de pair avec un autre instrument : l'analyse des risques. Tandis que la modélisation des menaces consiste à identifier les regards dont un utilisateur doit se cacher, l'évaluation des risques est un outil que les formateurs et les organismes de sécurité numérique utilisent pour analyser la probabilité qu'une menace se concrétise. Il devient important non seulement de savoir qui est l'adversaire dont on doit se cacher, mais aussi d'évaluer ses chances concrètes de se

[14] Peter Torr, « Demystifying the threat modeling process, » *IEEE Security & Privacy*, vol. 3, n° 5, 2005, pp. 66-70.

[15] Ebenezer A. Oladimeji, Sam Supakkul, and Lawrence Chung, « Security threat modeling and analysis: A goal-oriented approach, » *Proceedings of the 10th IASTED International Conference on Software Engineering and Applications (SEA 2006)*, 2006, pp. 13-15.

[16] https://ssd.eff.org/fr/glossary/threat-model

retrouver nez à nez avec lui. Si le risque est décrit comme une « traduction » culturelle du danger[17], l'évaluation du risque est une « quantification de l'incertitude »[18], qui le produit comme chose pouvant être « connue, atténuée, augmentée et diminuée, calculée »[19].

Les formateurs en sécurité numérique que nous avons interrogés au cours de cette étude en sont venus à voir la modélisation de menaces et l'analyse de risques comme de formidables outils pour cibler et structurer leurs sessions de formation. Plusieurs des sessions de formation que nous avons observées en Ukraine et en Russie ont fait usage de diverses techniques de modélisation des menaces. Par exemple, en introduction de la session « Sécurité numérique pour les militants » tenue à Saint-Pétersbourg, en Russie, le 10 avril 2016, P., le formateur, ouvrait avec ces mots :

> *Avant de commencer, on doit décider de qui on se protège. Tout d'abord, de l'État. Rien que l'année dernière, 200 procès ont été ouverts à cause de publications en ligne, de commentaires, etc. Ensuite, on doit se protéger des entreprises. Au risque de dire des évidences : il est clair que différentes sociétés accumulent des informations, et on nous fournit gratuitement beaucoup de services bien utiles, mais en échange ces sociétés s'approprient des informations sur nous. Troisièmement, il existe aussi d'autres agents malveillants qui aimeraient avoir accès à nos portefeuilles en ligne ou nous pirater juste pour le plaisir* (traduit du russe par nous-mêmes).

Cette division des adversaires en trois catégories n'était pas une simple figure rhétorique pour introduire la session de formation : elle a ensuite été utilisée tout au long des trois heures d'atelier, afin de regrouper autour de ces trois grandes catégories les différents outils de protection de la vie privée dont les élèves pourraient avoir besoin. Le fait de structurer une formation autour d'un adversaire en particulier signifie qu'il faut identifier non seulement les ressources techniques dont dispose un adversaire, mais aussi les paramètres extra-techniques – comme le contexte juridique, par exemple.

Les formateurs ukrainiens V. et M., tous deux spécialisés dans les utilisateurs à haut risque susceptibles d'être confrontés à des adversaires puissants, de niveau étatique, ou peut-être même à des menaces physiques, ont tenté une autre façon de structurer une session de formation. La formation, qui s'est tenue le 15 janvier 2017 à Kiev, incluait l'usage d'un tableau que les participants et les formateurs devaient remplir (figure 1.1).

---

[17] Mary Douglas and Aaron Wildavsky, *Risk and Culture*, Berkeley, University of California Press, 1982; Paulo Vaz and Fernanda Bruno, « Types of Self-Surveillance: from abnormality to individuals 'at risk' », *Surveillance and Society*, vol. 1, n° 3, 2003, pp. 272-291.

[18] Sun-ha Hong, « Criticising Surveillance and Surveillance Critique: Why privacy and humanism are necessary but insufficient », *Surveillance & Society*, vol. 15, n° 2, 2017, pp. 187-203.

[19] Theodore M. Porter, *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life.* Princeton, NJ, Princeton University Press, 1995.

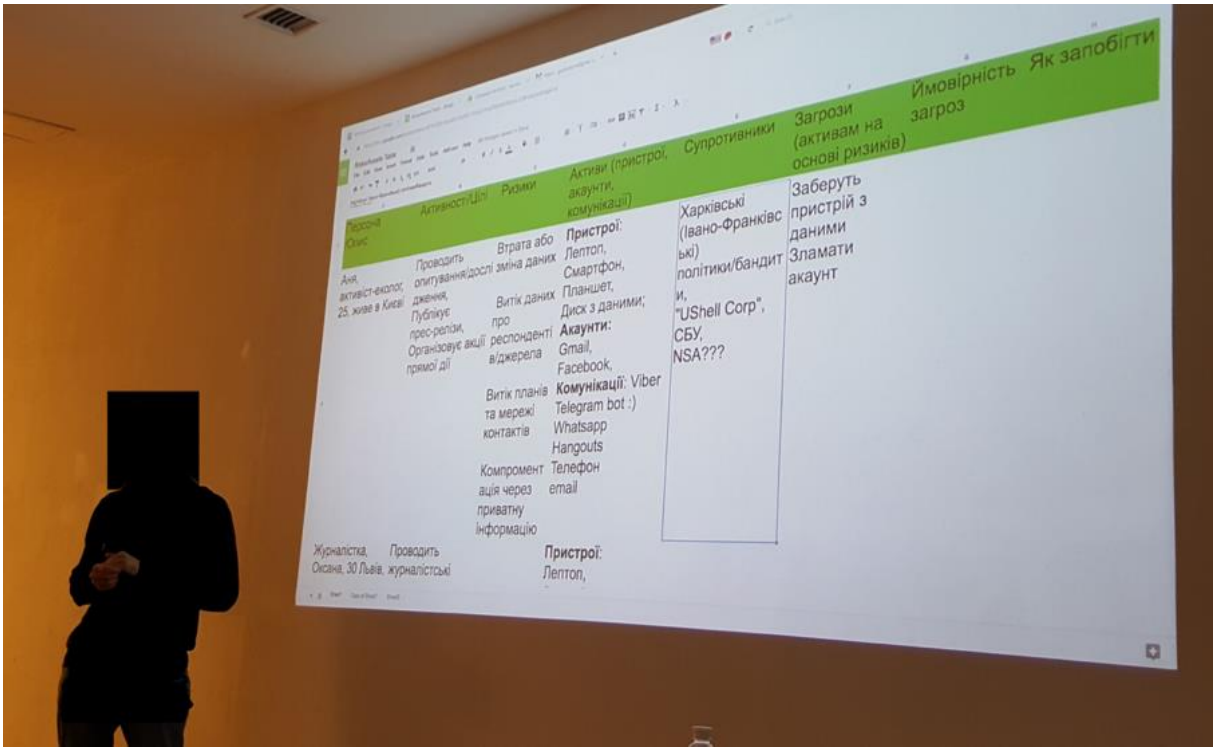

Fig. 1.1. Formation à la sécurité numérique observée à Kiev, en janvier 2017. Le tableau comprend les colonnes suivantes (de gauche à droite) : Description d'une personne, ses fonctions et activités, risques, « actifs » (appareils, comptes, types de communications utilisés), adversaires, menaces (appliquées aux actifs en fonction des risques), possibilité qu'une menace se produise, manières d'éviter les risques.

La formation était structurée autour de la construction collaborative de plusieurs profils fictifs (par exemple : Anya, 25 ans, militante écologiste ; Oksana, 30 ans, journaliste, etc.) et l'identification des actifs, adversaires et menaces qui leur correspondent. Ainsi, les formateurs ne se sont pas attachés à énumérer les outils existants pour améliorer la protection de la vie privée, mais à expliquer une méthodologie précise de modélisation personnalisée des menaces. Pour les formateurs, la capacité d'un utilisateur à analyser une situation et un contexte très concrets compte plus que sa connaissance avancée de plusieurs outils. Bien que certaines des sessions de formation observées aient néanmoins été centrées sur des démonstrations de certains outils en particulier, la plupart des formateurs critiquent globalement les approches centrées sur les outils et insistent plutôt sur l'importance de formation personnalisées, basées sur la modélisation des menaces :

> *Très souvent, les formations se transforment en formations aux outils. Mais dans notre travail, les outils ne sont pas notre préoccupation première, ni même seconde. Ce qui est primordial, c'est l'évaluation des besoins des participants, de ce qu'ils utilisent déjà. Et ce n'est qu'après que nous réfléchissons à ce que nous pouvons leur suggérer d'utiliser, et encore*

une fois, sans recommandations fermes, on ne va jamais dire : « vous n'avez besoin que de cet outil et c'est tout » [M., formateur en sécurité des systèmes d'information, Ukraine].

La communauté de la sécurité numérique est très réflexive quant à ses propres pratiques de formation et aux critères d'évaluation appliqués aux logiciels de messagerie sécurisée et aux clients de messagerie. Ces dernières années, le passage d'une approche centrée sur l'outil à une approche centrée sur l'utilisateur a constitué une sorte de changement de paradigme parmi les formateurs et les experts, qui considèrent de plus en plus les capacités de l'utilisateur à évaluer son propre modèle de menace comme étant cruciales. Comme le dit le célèbre guide de l'EFF « Surveillance Self-Defense »,

« Tenter de protéger toutes vos données, de tout le monde, en tout temps est irréaliste et épuisant. Mais n'ayez crainte ! La sécurité est un processus, et une planification réfléchie vous permettra d'établir un plan qui vous convient. La sécurité ne se réduit pas aux outils que vous utilisez ou aux logiciels que vous téléchargez. Elle commence par une compréhension des menaces particulières auxquelles vous êtes exposé et de la façon de vous en prémunir[20] ».

Cette « approche sur mesure » des modèles de menace dans les sessions de formation à la sécurité est d'autant plus importante que les développeurs dans le domaine de la messagerie sécurisée discutent actuellement d'un certain nombre de problèmes de cryptographie non résolus, tels que le stockage des métadonnées, les vulnérabilités des infrastructures centralisées, l'utilisation des numéros de téléphone comme identifiants, etc. En l'absence d'un « outil parfait » à tous ces égards, les formateurs recommandent des assemblages de différents outils et de pratiques de sécurité opérationnelle (« sécurité physique ») visant à minimiser les inconvénients des outils existants et présentant différentes caractéristiques, du chiffrement « en transit » au chiffrement « au repos », en passant par l'obfuscation des métadonnées, etc. La pratique de la modélisation des menaces aide à résoudre, et dans une certaine mesure à compenser, certains de ces problèmes techniques qui restent à résoudre.

Il est également important de noter que, pour un modèle de menace donné, des facteurs extra-cryptographiques tels que la facilité d'apprentissage d'un outil, la pression sociale ou l'effet de réseau (les nouveaux utilisateurs adoptant un outil parce qu'une masse critique d'individus l'utilise déjà) peuvent revêtir plus d'importance que l'efficacité technique d'un protocole cryptographique. Ainsi, un formateur en Ukraine donnait souvent à ses élèves utilisateurs à haut risque un conseil contre-intuitif de prime abord, mais finalement logique de son point de vue : il leur recommandait d'utiliser WhatsApp et Gmail plutôt que Signal ou une boite mèl chiffrée par PGP, car « tout le monde l'utilise déjà et sait comment ça fonctionne ». En d'autres termes, l'adoption de ces outils sera plus rapide et entraînera moins d'erreurs. Ainsi, le temps et la courbe d'apprentissage viennent s'ajouter aux facteurs affectant la propension des formateurs à recommander un outil.

[20] Voir https://ssd.eff.org/fr/module/votre-plan-de-s%C3%A9curit%C3%A9.

De « rien à cacher » à « parano complotiste », un continuum de niveaux de risque

En dehors des formateurs et des experts en sécurité numérique, les utilisateurs lambda développent aussi leurs propres méthodes pour évaluer leurs risques et inventent en conséquence des pratiques d'autodéfense numérique *ad hoc*. Cependant, même après les révélations de Snowden, une proportion conséquente des citoyens européens partage le sentiment de n'avoir « rien à cacher », et certains considèrent même le simple fait de dissimuler des traces en ligne comme un potentiel indice d'une éventuelle activité criminelle. Une étude récente a révélé un certain état d'apathie collective : « bien que les utilisateurs en ligne ressentent un malaise face à la collecte massive de leurs données personnelles et s'en préoccupent, le manque de compréhension quant à la manière dont ces données sont collectées ainsi qu'un sentiment d'impuissance conduisent à la résignation et à l'apathie du public »[21].

L'argument du « rien à cacher » a notoirement été rondement critiqué par la communauté de la sécurité, ce qui a donné lieu à la production d'une variété de contenus culturels et de tutoriels en ligne visant à sensibiliser le « grand public » à la sécurité numérique[22]. Ces contributions alimentent le débat actuel sur la frontière ténue qui sépare la surveillance ciblée de la surveillance de masse et les utilisateurs à haut risque des utilisateurs à faible risque. La limite entre se cacher des gouvernements et se cacher des entreprises devient également de plus en plus floue, au fur et à mesure que l'image de « l'adversaire » devient de plus en plus complexe et hybride[23].

Là où la grande majorité des études sur les utilisateurs dans le domaine de la *usable security* – le champ d'étude qui évalue la facilité d'utilisation de la sécurité numérique – ont été menées avec des sujets issus de la « population générale » (notamment des étudiants, en fait), les résultats de notre étude diffèrent légèrement en ce qui concerne la conscience et les préoccupations des utilisateurs en matière de vie privée. Nous avons classé les individus de notre population selon deux axes : leur degré de connaissances des technologies et leur situation en matière de risques. Nous avons ainsi obtenu quatre groupes, que nous examinerons tour à tour dans la suite de ce chapitre – même si cette distinction, bien que nous ayons pu la trouver utile sur le plan opérationnel, avait aussi ses limites, comme nous le verrons plus loin.

Si, chez les profils présentant une situation à faible risque mais possédant un haut niveau de connaissances techniques, la conscience des risques liés à la vie privée et à la sécurité était très élevée, les comportements de ces utilisateurs n'étaient en revanche généralement pas sûr dans l'ensemble : un

[21] Arne Hintz and Lina Dencik, « The politics of surveillance policy: UK regulatory dynamics after Snowden, » *Internet Policy Review*, vol. 5, n° 3, 2017. DOI: 10.14763/2016.3.424

[22] Citons, parmi les initiatives récentes, le documentaire *Nothing to Hide*: http://www.allocine.fr/video/player_gen_cmedia=19571391&cfilm=253027.htm

[23] Francesca Musiani, « Dangerous Liaisons? Governments, companies and Internet governance », Internet Policy Review, n° 2, vol. 1, 2013, DOI: 10.14763/2013.1.108

grand nombre de développeurs ou de formateurs techniques utilisaient des applications de messagerie électronique et de messagerie texte non chiffrées. Par exemple, alors que des études d'utilisabilité ont récemment montré que Telegram souffrait d'un certain nombre de problèmes graves en matière d'utilisabilité et de sécurité[24], le chiffrement pour les discussions de groupe étant très basique, les militants du Parti Pirate – qui sont développeurs et administrateurs systèmes et/ou réseaux – utilisent Telegram quotidiennement (le groupe Telegram du Parti Pirate Russie, par exemple, comptait 469 utilisateurs au 24 novembre 2019). Cependant, ces usagers ont également recours à d'autres tactiques d'autodéfense, comme l'autocensure (éviter de parler de certains sujets) et la pseudonymisation (éviter les vraies photos de profil et les noms d'utilisateur).

Cela peut surprendre, mais il n'y a pas de corrélation stricte, du moins dans nos entretiens, entre les modèles de menace des utilisateurs, leur niveau de connaissances techniques, les caractéristiques de sécurité d'un outil – comme la longueur de la clé ou l'algorithme de génération de la clé – et la dynamique d'adoption de cet outil. Au contraire, d'autres caractéristiques extra-cryptographiques et extra-sécuritaires peuvent devenir des arguments pour l'adoption d'un outil spécifique. Dans le cas de Telegram, il est intéressant d'observer la manière dont le protocole cryptographique réel et les propriétés de sécurité et de confidentialité passent au second plan dans les discours des utilisateurs, derrière les caractéristiques de l'interface et la réputation du créateur de l'application. D'après nos entretiens, la confiance en Telegram ne repose pas sur sa technologie, mais sur la personne qui la met en œuvre et sa position politique :

> Utilisateur 1 *: Peut-être que vous ne devriez pas discuter de cela sur Telegram ?*
>
> Utilisateur 2 *: Pourquoi pas ? Pashka Durov ne donnera jamais aucune de nos données, il n'a rien à faire de la police russe » [extrait d'une discussion en ligne sur un chat de groupe « Soprotivlenie* » [Résistance], posté le 11 juin 2017 ; traduit du russe par nous-mêmes].

Les membres de populations à haut risque disposant de peu de connaissance, cependant, n'avaient pas une conscience absolue des risques concernant les questions de vie privée (et n'étaient, par exemple, pas conscients de la nécessité d'utiliser des plugins de navigateur protégeant la vie privée), et accordaient davantage d'importance au comportement en matière de mèl et de messagerie instantanée. Bien que ces utilisateurs ne soient pas toujours en mesure de décrire clairement les vecteurs d'attaque possibles, ils avaient une image très multiforme et complexe de leur adversaire. Cette image a clairement pris forme dans les dessins que nous avons recueillis lors de nos entretiens et nos observations d'ateliers de formation, pour lesquels nous avions demandé aux répondants de représenter les personnes ou les entités qu'ils considéraient comme leur adversaire (figure 1.2).

[24] Ruba Abu-Salma, Kat Krol, Simon Parkin, Victoria Koh, Kevin Kwan, Jazib Mahboob, Zahra Traboulsi, and M. Angela Sasse, « The Security Blanket of the Chat World: A Usability Evaluation and User Study of Telegram, » in Internet Society (ed.), *Proceedings of the 2nd European Workshop on Usable Security (EuroUSEC)*, Paris, France, 2017.

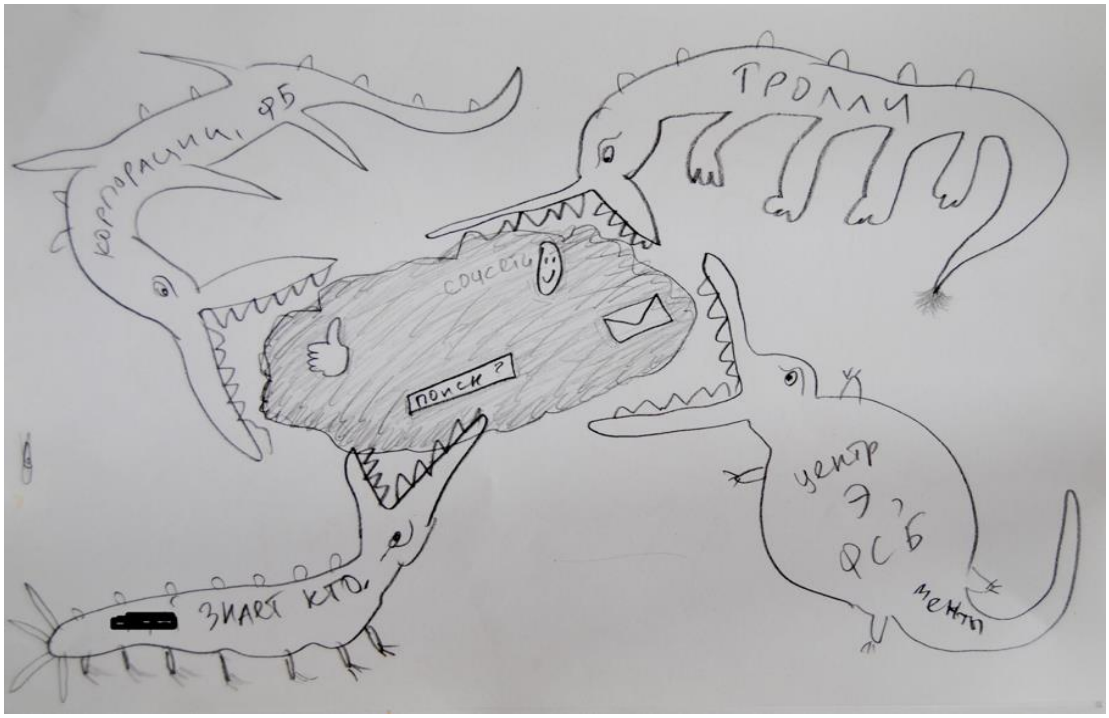

Fig. 1.2. Représentation des « communications en insécurité » par une utilisatrice. Dessin réalisé par une militante d'un collectif féministe, recueilli lors d'un atelier sur la sécurité numérique à Saint-Pétersbourg, en avril 2017. Les « crocodiles » sont étiquetés (dans le sens des aiguilles d'une montre en partant d'en haut à gauche) : « Grandes entreprises, Facebook » ; « Trolls » ; « Centre contre l'extrémisme, FSB, police » ; « P*tain, qui sait ? ». Sur le nuage : « Recherche » ; « Réseaux sociaux ».

Les utilisateurs « à faible niveau de connaissances et à haut risque » déploient de leur côté des méthodes spécifiques, souvent uniques et personnelles, pour protéger leurs communications et leurs informations, ce qui se traduit par un assemblage varié d'outils et de pratiques, tant dans leur comportement hors ligne (ingénierie sociale, sécurité opérationnelle « OPSEC ») qu'en ligne (figure 1.3).

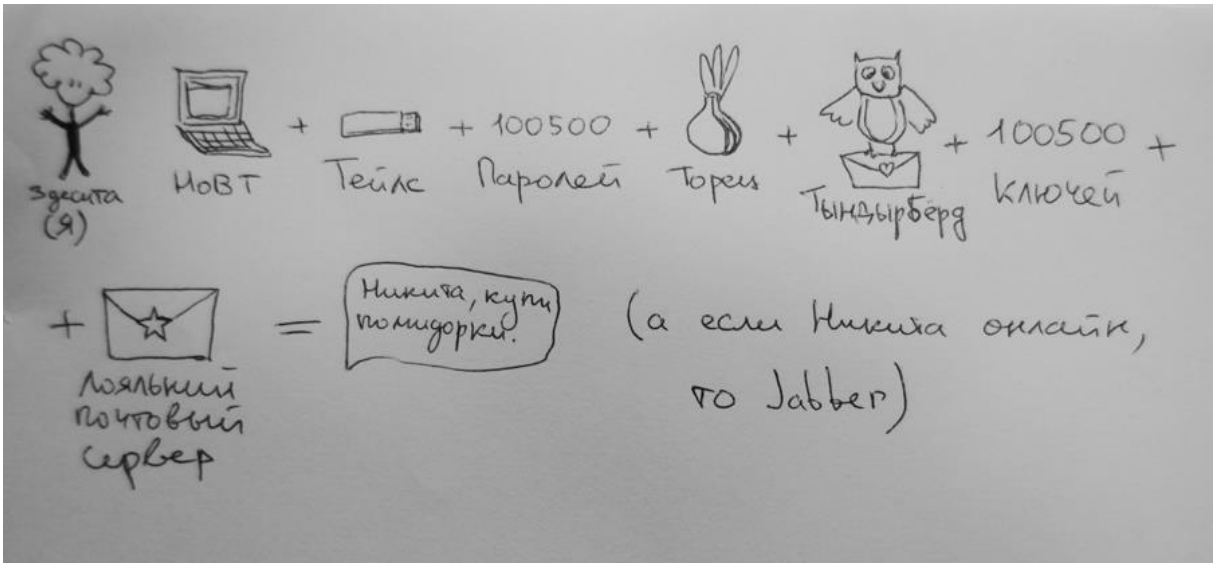

Fig. 1.3. Représentation des « communications sécurisées » par une utilisatrice militante antifasciste. Dessin recueilli lors d'un atelier sur la sécurité numérique à Saint-Pétersbourg, avril 2017. De gauche à droite : « Moi : ordinateur portable + Tails + 100500 mots de passe + Tor + Thunderbird + 100500 clés + messagerie de confiance = message « Nikita, pourrais-tu acheter des tomates s'il te plaît ? ». (Et si Nikita est en ligne, alors Jabber) »

Par exemple, les utilisateurs à haut risque en Russie et en Ukraine – à savoir, les militants de gauche qui ont fait l'objet de menaces policières et d'une surveillance ciblée entre 2012 et 2017 – utilisent souvent des services de « secrets uniques », des pastebins sensés détruire les messages aussitôt qu'ils ont été lus[25]. Ces usagers disent que la saisie de leurs appareils est la principale menace leur pesant dessus. Ils avancent donc qu'un lien autodestructeur est le moyen le plus sûr de communiquer, même si les liens vers ces sites sont souvent envoyés via des canaux non sécurisés, comme Facebook Messenger. En revanche, ces pratiques mènent aussi ces utilisateurs à haut risque à délaisser des applications *a priori* plus spécifiquement destinées aux militants.

La sécurité par compartimentation et le risque « relationnel »

Comme le montrent ces exemples, la multitude d'applications de messagerie reflète la variété des comportements des utilisateurs et des pratiques d'analyse des risques. En fait, les utilisateurs se perçoivent comme ayant plusieurs identités, dont chacune est susceptible de nécessiter ses propres

[25] Les services de ce type les plus communément utilisés sont One Time Secret (https://onetimesecret.com/) et Privnote (https://privnote.com/)

pratiques de soin de soi numérique et un ensemble d'outils spécifiques. Cela génère une forme de sécurité dite « par compartimentation ».

Les utilisateurs utilisent différentes applications de messagerie pour différents groupes de contacts, en fonction du niveau de risque perçu. Certaines des personnes faisant face à un niveau de risque élevé à qui nous avons parlé disaient utiliser WhatsApp ou Facebook Messenger pour le travail et les relations familiales, tout en préférant le courrier électronique crypté PGP, Signal ou Privnote pour les contacts militants. Certains préfèrent transférer toutes les communications vers une seule application, mais disent avoir du mal à convaincre leurs proches de changer de comportement en ligne (le fameux « problème de la migration numérique ») ou se heurter à des problèmes de compatibilité (par exemple, Signal ne fonctionne pas sur les anciens téléphones).

Par conséquent, le risque est un concept relationnel dès lors qu'il est appliqué à la sécurité numérique, car il dépend fortement des graphes sociaux et des contextes de communication de l'usager. Comme l'explique cet utilisateur ukrainien à haut risque, impliqué dans un collectif de soutien aux prisonniers politiques :

> *Mon risque est toujours lié au risque d'autres personnes. Je ne veux pas utiliser mon téléphone portable pour me connecter à mon compte militant, car il sera possible de relier les deux. Et même si je pense que je n'ai rien fait, d'autres personnes ont des raisons de se cacher. Et puis... je ne sais jamais quand quelqu'un va s'en prendre à moi. Il n'est pas sage de prédire l'avenir. Juste avant son arrestation, Khodorkovsky disait aussi que personne ne s'intéressait à lui.*

En ce sens, même s'il peut être utile de catégoriser les utilisateurs le long des axes que nous avons utilisé – cela facilite, par exemple, l'application de traitements statistiques à nos données, ce que les technologues de l'équipe NEXTLEAP ont beaucoup apprécié et nous a permis de co-écrire quelques articles avec eux – la différence entre les utilisateurs à faible risque et les utilisateurs à haut risque est en fait très dépendante du contexte, et toujours changeante : au contact de personnes à haut risque, une personne à faible risque doit augmenter son niveau de sécurité et peut elle-même devenir à haut risque. Un utilisateur autrichien, organisateur de festival s'identifiant comme une personne à faible risque, formulait cette idée ainsi :

> *Je travaille pour un festival dont le but est de générer du rayonnement. Et je m'adapte aux personnes que j'invite ou avec qui j'élabore des projets. Le risque de ma communication est donc lié au risque pris par mes interlocuteurs. Donc, par exemple, avec [X], [Y][26] ou d'autres, je crypte toujours tout, bien sûr, et je vérifie toujours que l'interlocuteur que j'invite possède une clé publique sur un serveur de clés, de sorte que je commence à communiquer de manière cryptée [...] Ennemi ? Beaucoup des orateurs que j'invite ont de sérieux ennemis ; je m'adapte donc à cela.*

[26] Il s'agit de deux activistes connus dans le champ de la technologie et de la défense des droits humains.

Cette approche de la sécurité par la « compartimentation » se traduit également par des bricolages sur le plan matériel, allant de la pratique la plus populaire du « dual-booting » (combiner un système d'exploitation « activiste » et un système d'exploitation « normal » sur la même machine), à des solutions plus sophistiquées de cachette ou de système d'exploitation dissimulé. Ces comportements d'utilisateur et ces pratiques de « sécurité par la compartimentation » ont été récemment incorporés *à la conception* d'un projet appelé Qubes. Il s'agit d'un système opérationnel basé sur une multitude de machines virtuelles créant des environnements de travail isolés qui permettent aux utilisateurs de coordonner et de gérer les « parties » de leur identité en ligne, avec leurs divers besoins et leurs différentes exigences de sécurité.

Cependant, les risques et les modèles de menace évoluent également dans le temps. Ils dépendent non seulement des réseaux relationnels des utilisateurs, mais aussi des réactions et des comportements supposés de « l'adversaire ». Ainsi, pour cet utilisateur grec à haut risque et à haut niveau de connaissances, il est important de réinventer constamment ses pratiques de sécurité quotidiennes :

> *Selon l'acte ou ce que je fais, j'ai un OPSEC spécifique. Je retiens les principales étapes par cœur, bien que je n'utilise pas les mêmes pratiques à chaque fois car, une fois utilisée, chaque méthodologie est grillée. Selon l'endroit, j'essaie de singer les pratiques courantes dans le coin plutôt que d'improviser aveuglément. L'adversaire en apprend toujours plus en m'observant et en surveillant des personnes de confiance ou des amis qui ne sont pas assez prudents.*

Si la distinction entre risque élevé et risque faible est à prendre avec un grain de sel, il en va de même pour les définitions des données sensibles et non-sensibles. La religion, la moralité, le genre deviennent des paramètres importants pour influencer la définition d'une « information sensible ». Nos entretiens avec des utilisateurs au Moyen-Orient, par exemple, montrent que les femmes musulmanes doivent notamment se cacher de leurs propres compagnons ou de membres de leurs familles, qui constituent un adversaire de premier plan. Comme l'explique l'une de nos interlocutrices, une femme Iranienne de 27 ans, des photos d'un mariage non-religieux peuvent devenir aussi sensibles qu'une critique politique et présenter des risques importants pour la personne qui les partage. Ce n'est donc pas le type d'information qui définit en soi la catégorie « à haut risque », mais le contexte plus général dans lequel opère l'utilisateur : ainsi, les modèles de menace et les niveaux de risque peuvent dépendre du genre et de la culture.

« Si tu utilises cet outil, c'est que tu as quelque chose à cacher » : les paradoxes de l'adoption massive du chiffrement

Sur notre terrain, il était moins questions d'open-source et de choix de licence dans les sessions de formation pour les usagers à haut risque, car ceux-ci n'associent pas toujours l'open-source à la sécurité. L'open-source est perçu comme un critère moins important dans le contexte d'une menace

physique immédiate : si une solution propriétaire mais « efficace » et « facile à expliquer » existe, les formateurs lui donneront la priorité. Par exemple, en Ukraine, WhatsApp est l'application la plus recommandée, car elle est considérée comme facile à installer. Les formateurs accordent moins d'importance à la licence propriétaire de WhatsApp et à sa collaboration avec Facebook (notamment en ce qui concerne le partage des métadonnées) qu'aux perceptions des utilisateurs en matière de sécurité. Leur but premier, dans les contextes à haut risque avec des utilisateurs peu informés, est d'aider ces utilisateurs à abandonner rapidement les outils non chiffrés, ainsi que les outils dont les créateurs sont susceptibles de collaborer avec leurs adversaires.

> *Depuis que WhatsApp a adopté le chiffrement de bout en bout, nous ne passons généralement plus autant de temps sur le chiffrement des messageries instantanées [pendant les formations], et nous recommandons de rester sur WhatsApp si les gens l'utilisent déjà. Ainsi, ils peuvent continuer à communiquer avec tous leurs amis, et aussi... cela leur semble familier, et cela ne les choque pas. Et les gens disent [pendant les formations] que s'ils utilisent WhatsApp, c'est moins suspect que s'ils utilisent une application spéciale pour les militants* [I., formatrice en sécurité informationnelle, Ukraine].

Cette citation soulève une préoccupation importante qu'ont abordée un certain nombre de nos interlocuteurs et que nous avons pu observer lors d'évènements CryptoParty et de formations à la sécurité informationnelle : *est-ce que le fait même d'utiliser une application conçue pour les activistes ne constitue pas une menace en soi* ? Cela fait référence à la fameuse « théorie du chat mignon de l'activisme numérique » d'Ethan Zuckerman[27], selon laquelle il est plus sûr et plus facile pour les activistes d'utiliser les mêmes plateformes grand public qui sont utilisées pour partager des photos de « lolcats », tandis que les usagers d'un outil estampillé « activiste » risquent de se voir placés sous une surveillance ciblée (et donc plus aisée et moins chère).

Cette préoccupation révèle une anxiété partagée (mais souvent sous-explorée) parmi les utilisateurs à propos de certains types de métadonnées – même si ce terme particulier n'est pas toujours utilisé explicitement – comme, par exemple, les données concernant l'installation de certaines applications. Une copieuse critique de tous les outils existants nous a souvent été opposée dans nos entretiens, qu'ils soient avec des formateurs en sécurité informatique ou des utilisateurs non techniques. Cela fait écho aux résultats d'une autre étude récente sur l'utilisabilité des outils de chiffrement de bout en bout, qui concluait que « la plupart des participants ne pensaient pas les outils sécurisés capables d'offrir une protection contre des adversaires puissants ou bien informés »[28]. Parmi les raisons de ne pas adopter le chiffrement, de nombreux utilisateurs ont cité le fait que l'utilisation d'outils spécifiques exposerait

---

[27] Zuckerman, Ethan. 2008. "The Cute Cat Theory Talk at ETech", *My Heart's In Accra*, March 8. http://www.ethanzuckerman.com/blog/2008/03/08/the-cute-cat-theory- talk-at-etech

[28] Abu-Salma et al., cit., p. 2

leurs graphes sociaux et leur style de vie « militant » à leurs adversaires. Un utilisateur russe a également évoqué l'effet inverse – l'utilisation d'un outil conçu pour les activistes comme moyen de « gagner leur confiance » – en racontant l'histoire d'un policier infiltré qui a utilisé un compte de messagerie @riseup.net comme moyen d'intégrer la liste de diffusion d'un mouvement étudiant pendant les grandes manifestations de 2011-2012.

La plus pure expression de ce « scepticisme à l'égard des outils » est illustrée dans un dessin réalisé par l'une des personnes interrogées – un correspondant de guerre européen travaillant dans des situations à haut risque au Moyen-Orient – lorsqu'on lui a demandé de dessiner une représentation de son adversaire (figure 1.4).

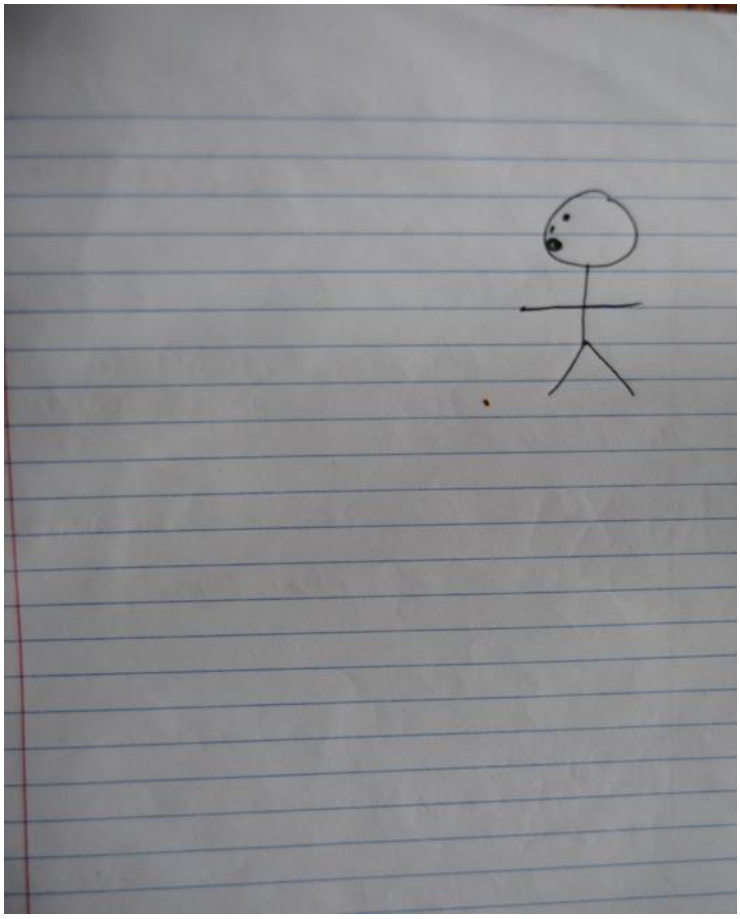

Figure 1.4. Dessin recueilli lors de l'entretien du 16 février 2017.

L'utilisateur commentait le dessin ainsi :

> *Dans le cas d'une communication réellement sécurisée, je dis quelque chose mais personne ne sait ce que j'ai dit ni à qui [...] j'aurais pu simplement vous donner une feuille blanche, qui aurait signifié qu'aucune trace d'un acte de communication n'est visible. Mais dès lors que vous m'avez demandé de vous dessiner quelque chose...* [C, homme, journaliste, haut risque].

L'adoption du cryptage par les applications de messagerie classiques (par opposition aux applications destinées plus spécifiquement aux activistes) entraîne un effet particulier que l'un de nos

répondants résumait en utilisant l'expression « un poisson dans la mer » (au sens d'être « une entité parmi tant d'autres comme elle » dans un grand espace, et de se protéger mutuellement en se dissimulant mutuellement) :

> *Imaginez que je n'ai rien à cacher, mais que j'utilise quand même une application cryptée de bout en bout, alors les gens qui ont besoin de se cacher... comme les lanceurs d'alerte par exemple... il leur sera plus facile, disons, de disparaître dans ce grand flux de photos de chats ou de messages d'amour. J'ai donc l'impression d'aider quelqu'un lorsque j'utilise le cryptage en permanence pour toutes mes communications* [Utilisatrice à faible risque, journaliste technique, Autriche].

Un phénomène intéressant de « responsabilité partagée » découle de cette adoption massive du chiffrement : le plus les outils de chiffrement de bout-en-bout ont d'utilisateurs, plus ils deviennent sûrs à utiliser pour tous, mais tout particulièrement pour les utilisateurs dont la vie et la liberté dépendent de ces outils. Alors qu'il existe une réelle corrélation technique entre le nombre d'utilisateurs et le degré de protection de la vie privée lors de l'adoption massive d'applications distribuées ou peer-to-peer, les conséquences de l'adoption massive d'applications centralisées (comme Signal et WhatsApp) ou du chiffrement des e-mails sont souvent décrites comme une augmentation du degré de difficulté humaine et technique que l'adversaire devra surmonter afin d'atteindre ses objectifs de surveillance :

> *Plus les gens utilisent le chiffrement, plus il sera coûteux pour les gouvernements de tout lire. Il ne s'agit pas d'atteindre une sécurité à 100%... Ça n'existe tout simplement pas ! Il s'agit de leur faire perdre leur temps et leur argent pour décrypter nos affaires, et à la fin ils lisent quelque chose comme « Et si on allait manger une pizza ce soir » ...* [formateur en sécurité informatique, Ukraine].

Même si la collaboration de Moxie Marlinspike, développeur en chef de Signal, avec WhatsApp et Facebook était controversée et sujette à des critiques dans un certain nombre de cercles technophiles – en particulier dans les communautés F/OSS (*Free and Open Source Software* : Logiciel Libre) – l'adoption massive du chiffrement de bout en bout a eu un impact important sur la gouvernance d'Internet. Grâce à des applications telles que WhatsApp, qui ont démocratisé la cryptographie forte, la thèse du « chiffrement en tant que droit humain » et la demande pour un « accès égal au chiffrement » se sont généralisées. Parmi les initiatives récentes, une lettre était signée par 65 ONG axées sur la protection de la vie privée (dont Privacy Now, EFF et Article 19) et adressée à l'ONU en 2017 pour demander la dépénalisation des utilisateurs de technologies de protection de la vie privée et des formateurs en sécurité numérique. Deux ans plus tôt, le rapporteur spécial des Nations unies sur les droits de l'homme présentait la vie privée et le droit au secret de la correspondance comme une composante essentielle de la liberté d'opinion et d'expression :

> *Dans des époques marquées par le terrorisme, les débats sur le chiffrement et l'anonymat se sont bien trop souvent concentrés uniquement sur leur potentielle utilisation à des fins*

criminelles. Mais les situations d'urgence ne dispensent pas les États de leur obligation de veiller au respect du droit international en matière de droits humains [...] Il faut que soit mise en évidence, dans le débat en général, la protection qu'offrent le chiffrement et l'anonymat, et tout particulièrement celle qu'elle offre aux groupes les plus exposés aux ingérences illégales[29].

Lors de nos entretiens, les développeurs et les formateurs en sécurité informatique ont souligné l'urgence de trouver une solution fiable au problème de la collecte des métadonnées. Comme nous l'avons déjà laissé entendre, il s'agit d'un domaine clé où les débats autour du chiffrement revêtent une nouvelle pertinence. Les métadonnées sont des données qui décrivent – ou fournissent des informations sur – d'autres données, telles que des conversations sur les réseaux sociaux, des échanges de courriels ou des transactions en ligne. Les appareils et les systèmes connectés à internet (ou prenant en charge son fonctionnement), y compris les systèmes de messagerie et autres systèmes de communication en ligne, collectent ces « informations sur les informations ». Une fois agrégées, celles-ci peuvent rendre compte non seulement des activités quotidiennes en ligne d'un utilisateur, mais aussi de celles d'autres utilisateurs et des activités de cet utilisateur dans la vie réelle. La collecte de métadonnées est particulièrement problématique, ou du moins peut l'être, car elle se fait en arrière-plan et à des fins diverses, et les utilisateurs ne peuvent généralement accéder qu'à une infime fraction des métadonnées collectées à leur sujet. Les controverses autour de la collecte de métadonnées sont nombreuses, notamment en ce qui concerne le consentement éclairé, le niveau de transparence vis-à-vis de l'utilisation ou du partage de ces données, l'existence de politiques de conservation (documents stipulant combien de temps une entité stockera les métadonnées) et la possibilité légale d'une collecte en masse ou sans mandat, en particulier par les agences gouvernementales[30]. En fin de compte, les développeurs et les formateurs semblent partager un consensus sur le fait qu'il n'existe actuellement aucune solution dans le domaine des applications de messagerie instantanée chiffrée de bout en bout qui offre réellement une bonne protection des métadonnées. Les développeurs et les formateurs associent la fuite de métadonnées à la centralisation :

Les métadonnées vous connectent bizarrement avec d'autres personnes et, pour des raisons technologiques, elles contiennent plus de sens que les données elles-mêmes [...] Aucune application de messagerie n'essaie de résoudre ce problème. Au lieu de ça, ils vous proposent de synchroniser vos carnets d'adresses pour savoir exactement à qui vous parlez, alors même que vous leur faites confiance pour que ça se retrouve dans des hashes ou je ne sais quoi. C'est le problème que les applications ne résolvent pas, ça ne va qu'en s'aggravant. Et on a

[29] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, published on May 22, 2015 and presented on June 17, 2015 https://www.eff.org/deeplinks/2015/06/strong-encryption-and-anonymity-are-guardians-free-expression

[30] Piscitello, D. (2016). Metadata Collection and Controversy. ICANN Blog, 27 June 2016, https://www.icann.org/news/blog/metadata-collection-and-controversy

maintenant des serveurs centralisés qui deviennent des honeypots, et ce n'est pas une question de données, mais de métadonnées. [Peter S., Heml.is].

« En fait… *In Google We Trust* » ? : Une remise en question de la dichotomie vie privée-sécurité

Quand nous avons tenté d'interpréter notre travail de terrain pour la première fois, notre hypothèse était que des modèles de menace très distincts pouvaient être associés à des types d'utilisateurs distincts, regroupés en fonction de leur statut de risque : « élevé » ou « faible ». Comme nous l'avons déjà remarqué, cette hypothèse était utile d'un point de vue opérationnel, notamment pour notre travail conjoint avec des informaticiens plus habitués aux études d'utilisabilité. Cependant, notre travail de terrain a montré les limites de cette dichotomie, en démontrant la relativité de deux visions binaires : les utilisateurs pouvaient être catégorisés non seulement comme étant à haut risque ou à faible risque, mais aussi en fonction de leurs préoccupations en matière de vie privée ou de sécurité. En fait, comme nous le verrons plus en détail dans la suite de cette section, ces deux préoccupations et les pratiques défensives qu'elles suscitent s'entremêlent.

En effet, parmi les personnes interrogées, les citoyens des pays supposés « à faible risque » (des pays occidentaux en démocratie stable) étaient plus préoccupés par les questions liées à la vie privée, tandis que les individus « à haut risque » (c'est-à-dire, dont l'appartenance à des groupes sociodémographiques particuliers leur vaut l'attention de régimes autoritaires) se concentraient sur des besoins urgents et des situations de vie ou de mort, et adoptaient souvent des solutions techniques plus faciles à installer et à utiliser (comme WhatsApp, par exemple), quand bien même leurs niveaux de protection de la vie privée laisserait à désirer. Les différentes attitudes envers les géants de la technologie, tels que Google, Apple, Facebook, Amazon et Microsoft, en sont un exemple. Les critiques à l'égard de ces entreprises émanent surtout d'utilisateurs occidentaux ayant un niveau élevé de connaissance des technologies de l'information et de leur socio-économie. En revanche, plusieurs utilisateurs « à haut risque » partagent l'idée que des services centralisés et quasi-monopolistiques comme Gmail, par exemple, présentent un meilleur rapport sécurité-utilisabilité. Les usagers opérant dans un contexte de fort risque et d'urgence ont tendance à chercher un compromis entre la convivialité et la sécurité, tandis que les utilisateurs techniquement expérimentés à faible risque se concentrent souvent davantage sur le développement de boîtes à outils véritablement complexes et multicouches pour préserver la confidentialité et la sécurité.

Cependant, certaines critiques des pratiques des géants de la technologie ayant émergé au sein de la communauté F/OSS ont atteint des cercles plus grand public, non techniques, dans des pays à haut risque. C'est le cas de la controverse sur la dépendance de Signal à l'égard de Google Play et de

Google Services[31], qui est apparue dans les cercles du logiciel libre avec le lancement – puis, promptement, l'abandon – du projet LibreSignal[32]. La dépendance de Signal à l'égard de Google est devenue problématique pour une communauté bien précise d'utilisateurs soucieux du respect de la vie privée et férus de technologie, qui optent pour des alternatives décentralisées aux outils de communication fournis par les géants du Net. Dans ce contexte, le choix d'une messagerie « sans Google » peut également être perçu comme un choix de « style de vie ». Ce choix va souvent de pair avec des choix de matériel alternatifs (comme un téléphone Linux, un Fair Phone, Copperhead OS, ou d'autres outils de protection de la vie privée). Comme le dit un utilisateur féru de technologie :

> *Si je n'aime pas le courant dominant dans les médias, si je n'aime pas le courant dominant dans la musique - pourquoi aimerais-je le courant dominant sur mon ordinateur ?* » [Daniel, fournisseur de services de messagerie, organisateur de festivals].

Toutefois, nos entretiens montrent que la dépendance de Signal à l'égard de Google Play a sérieusement affecté non seulement les utilisateurs avertis issus d'environnements présentant *a priori* peu de risque, mais aussi des utilisateurs vivant dans des contextes problématiques et disposant de peu de connaissances techniques. En Syrie, par exemple, le blocage de Google Play dans tout le pays a bloqué l'accès simple et rapide à l'application Signal pour les utilisateurs peu avertis, qui n'avaient pas les compétences nécessaires pour chercher d'autres moyens de l'acquérir. Les décisions techniques prises par les développeurs de technologies de protection de la vie privée – telles que les dépendances à l'égard de bibliothèques tierces et les choix en matière de licences et de protocoles – ne sont pas seulement une question de préférence ou de style de vie pour les utilisateurs, mais peuvent également avoir un impact sur leur sécurité dans des contextes où ils sont en danger de mort.

Les utilisateurs dans des contextes à « haut risque » ont également évoqué l'importance pour leurs modèles de menace de la question des réseaux décentralisés, autrefois considérée comme une préoccupation essentiellement « haute technologie, faible risque ». A titre d'exemple, nous avons pu observer dans nos récents échanges avec des militants de gauche russes et ukrainiens la volonté croissante de ces groupes de gérer leurs propres infrastructures de stockage de fichiers et de communication décentralisée.

Conclusions. Le risque est relationnel, la modélisation des menaces est cruciale

En fournissant un certain nombre d'exemples en lien avec les contextes d'utilisation, les besoins perçus des utilisateurs et la sélection d'outils potentiellement adéquats, nous avons montré dans ce

[31] https://github.com/WhisperSystems/Signal-Android/issues/127
[32] https://github.com/LibreSignal/LibreSignal

chapitre que, dans le domaine des communications en ligne et plus particulièrement de la messagerie sécurisée, le risque est relationnel, et qu'il est donc crucial de modéliser ses menaces afin de choisir le bon outil pour protéger ses communications. Par exemple, si l'objectif premier d'un utilisateur est de se cacher de son propre gouvernement, cet objectif sera inextricablement lié à l'évolution des habitudes de consommation et à la migration hors de plateformes propriétaires dont les modèles d'affaires reposent sur les données des utilisateurs. Dans ce contexte, « l'adversaire » ressemble à un réseau en constante évolution, fluide et connecté à des infrastructures privées et institutionnelles, plutôt qu'à une entité unique dotée de capacités bien définies et d'un ensemble prédéterminé de techniques et d'outils de surveillance et d'attaque.

Les formateurs et les organismes de sécurité numérique s'orientent vers une approche centrée sur les utilisateurs et donc vers des sessions de formation sur-mesure. En même temps, ils font de plus en plus face au défi de devoir expliquer à leurs stagiaires que les outils de protection de la vie privée ne garantissent pas à eux seuls une sécurité absolue. Les défis cryptographiques non résolus, tels que l'élaboration de solutions utilisables pour la préservation des métadonnées, sont en quelque sorte « compensés » par un patchwork de techniques de sécurité opérationnelles et une combinaison d'outils que les utilisateurs inventent et modifient en permanence. Ainsi, l'acte d'identifier « de qui il faut se cacher » – les processus de modélisation de menaces et d'analyse des risques – est un processus en constante évolution qui dépend d'un vaste ensemble de paramètres souvent non-techniques ou non-cryptographiques, tels que le graphe social de l'utilisateur, son genre, ses normes religieuses ou éthiques, sa profession, sa situation géopolitique et le régime politique de son gouvernement, ou la réputation et le charisme des créateurs de logiciels. En effet, la communication chiffrée est à la fois produite par – et le catalyseur du changement de – un vaste réseau comprenant des institutions (ou des acteurs se positionnant en opposition ou en résistance à celles-ci) et, bien sûr, une myriade d'infrastructures et de dispositifs techniques qui intègrent des concepts tels que la sécurité et la vie privée (voir notre précédent commentaire sur la gouvernance d'internet en introduction).

Aussi utile qu'elle puisse être sur le plan opérationnel pour le chercheur en tant qu'outil méthodologique pratique afin de constituer un échantillon diversifié d'utilisateurs pour les entretiens, la distinction entre risque élevé et risque faible montre des limites intrinsèques, principalement en raison de la nature « relationnelle » du risque que nous avons introduite dans ce chapitre. Pour peu qu'un utilisateur à faible risque ait au moins un utilisateur à haut risque dans son graphe social, il deviendra susceptible d'adopter un niveau de protection plus élevé, et même d'installer un outil spécifique pour communiquer avec ce contact. Inversement, dans certains contextes socio-politiques, des données qui seraient généralement considérées comme présentant un faible risque et n'étant pas sensibles peuvent en fait placer leurs propriétaires dans des catégories à plus haut risque. Si la conception d'outils de protection de la vie privée nécessite en effet d'imaginer le « pire des mondes possibles », il pourrait bien s'agir du monde d'un individu parmi nos contacts : la personne qui a le plus besoin de se cacher.