

Le *black fax* et ses dérivés

Nicolas Nova & Félicien Goguey

Le thème de la panne a fait l'objet de récentes publications (Bourrier & Nova 2019 ; Lambert & Raveux 2020), mais l'instrumentalisation des pannes y demeure en angle mort. Tirer parti des incidents, exploiter des bugs et détourner le fonctionnement des machines sont pourtant choses courantes dans les sociétés contemporaines. Ces stratégies individuelles comme collectives visent à interrompre un cours d'action, à regagner des marges, ou simplement, à protester.

Le noircissement de fax (*black fax*) est un cas notable de ce répertoire d'action, qui vise à provoquer la panne à distance. Il repose sur la possibilité de saturer les télécopieurs d'une organisation donnée en envoyant des centaines de pages sombres, dont l'impression en masse rend inutilisable l'appareil attaqué. L'afflux de pages uniformément noires vide les cartouches d'encre ou consomme le papier thermique et, en retour, empêche l'usage de la machine. Utilisé à la fois comme farce, en complément des canulars téléphoniques, et comme moyen de protestation dans des conflits asymétriques, le *black fax* a été employé par les Anonymous contre l'Église de Scientologie, par les Gilets jaunes contre le gouvernement français et des mairies, mais aussi par des syndicalistes lors de luttes sociales en entreprise. Le noircissement de fax a constitué une tactique permettant à des groupes d'activistes minoritaires de provoquer rencontres et négociations. Si l'usage du télécopieur s'est considérablement réduit avec l'avènement d'autres technologies de transmission d'information, le *black fax* reste vivace dans la dernière décennie, en particulier au sein des collectifs de hackers se réclamant du mouvement Anonymous.

Cette pratique de sabotage de la télécopie analogique trouve un prolongement dans le champ du numérique avec les attaques « par déni de service » (*Denial of Service* ou *DoS*). Celles-ci visent à perturber ou à paralyser temporairement le fonctionnement d'un serveur informatique en le « bombardant » de requêtes superflues, pour empêcher l'accès aux utilisateurs légitimes. Si les premières attaques par *DoS* étaient le fait de *hackers* solitaires œuvrant à partir d'une seule machine, la technique a rapidement évolué et recourt désormais à la puissance cumulée d'un grand nombre d'ordinateurs « zombies » (des *botnets*, mot-valise associant *robot* et *network*), préalablement infestés par un logiciel malveillant à l'insu de leurs propriétaires et commandés à distance. Ces attaques « par déni de service distribué » (*Distributed Denial of Service* ou *DDoS*), d'abord utilisées par des pirates informatiques comme des démonstrations de force destinées à gagner le respect de leur communauté, ont vite été adoptées comme moyen de représailles, de chantage voire d'extorsion.

Une tactique inverse consiste à perturber le fonctionnement des dispositifs de surveillance ou à brouiller leur manière de surveiller. Ainsi, la technique dite d'« obfuscation » procède par diffusion massive d'informations (le plus souvent erronées) afin de cacher l'information véritable et pertinente. Cette technique peut, elle aussi, être utilisée à des fins de protestation. Le plug-in de messagerie ScareMail, de Ben Grosser, permet par exemple d'ajouter dans la signature des emails un message menaçant, généré à partir de dictionnaires de mots-clés censés alerter et troubler la surveillance mise en place par l'agence étasunienne NSA. Le projet Masquerade de Félicien Goguy repose sur le même principe. Un programme envoie continuellement sur le réseau Internet des messages reconnus comme suspects par les programmes de surveillance, afin de perturber leur fonctionnement. Masquerade tente de déclencher des « faux positifs » dans les algorithmes de surveillance, en altérant la prise de décision entre deux possibilités (positif et négatif). Le principe ici n'est pas de cacher d'éventuelles informations, mais plutôt de manifester son désaccord face à la surveillance de masse mise en place par les États.

Toutes ces tactiques créent des perturbations dans la routine d'un système technique, en détournant les modalités de fonctionnement des objets qui le composent. Si l'envoi massif de fax noircis paraît aisé pour des activistes non-technophiles, les attaques contre les serveurs informatiques nécessitent un minimum de savoir-faire, ce qui interroge la reproductibilité de telles tactiques de protestations. Le projet *CV Dazzle* d'Adam Harvey, qui cherche à tromper ou éblouir les caméras de surveillance au moyen de maquillages, de coupes de cheveux et de vêtements lumineux, nous montre cependant que les techniques de luttes et de protestations de l'aire numérique savent se réinventer en restant appropriables par chacun.

Fig. 1 : Félicien Goguy, Masquerade, 2015-2019. Logiciel, BeagleBones Black, switch, imprimante matricielle, papier listing, MDF, acrylique. ©Dylan Perrenoud

Références

Bourrier M. & N. Nova 2019 « (En)quêtes de pannes », *Techniques&Culture* 72 (En cas de panne) : 12-29.

Lambert G. & O. Raveux 2020 « Pannes et accidents, mises en question et révélateurs des relations entre techniques, économie et société (XIX^e-XXI^e siècle) », *Artefact* 11 : 9-18.

Auteurs

Nicolas Nova est un anthropologue actif dans le domaine du design d'interaction, de la prospective et des cultures numériques. Il est à la fois professeur associé à la Haute école d'Art et de Design (HEAD – Genève) et co-fondateur du Near Future Laboratory,

une agence de prospective.

Félicien Goguey est artiste et designer d'interaction. Il poursuit sa thèse de doctorat entre la HEAD – Genève et le Laboratoire des humanités digitales à l'École polytechnique fédérale de Lausanne où il développe un travail de recherche basé sur la pratique autour d'un objet de surveillance : l'**intercepteur d'IMSI** (International Mobile Subscriber Identity).

Nova, N. & F. Goguey 2020 Le black fax et ses dérivés, *Techniques&Culture* 74, "Techniques de lutte", p. 150-151.