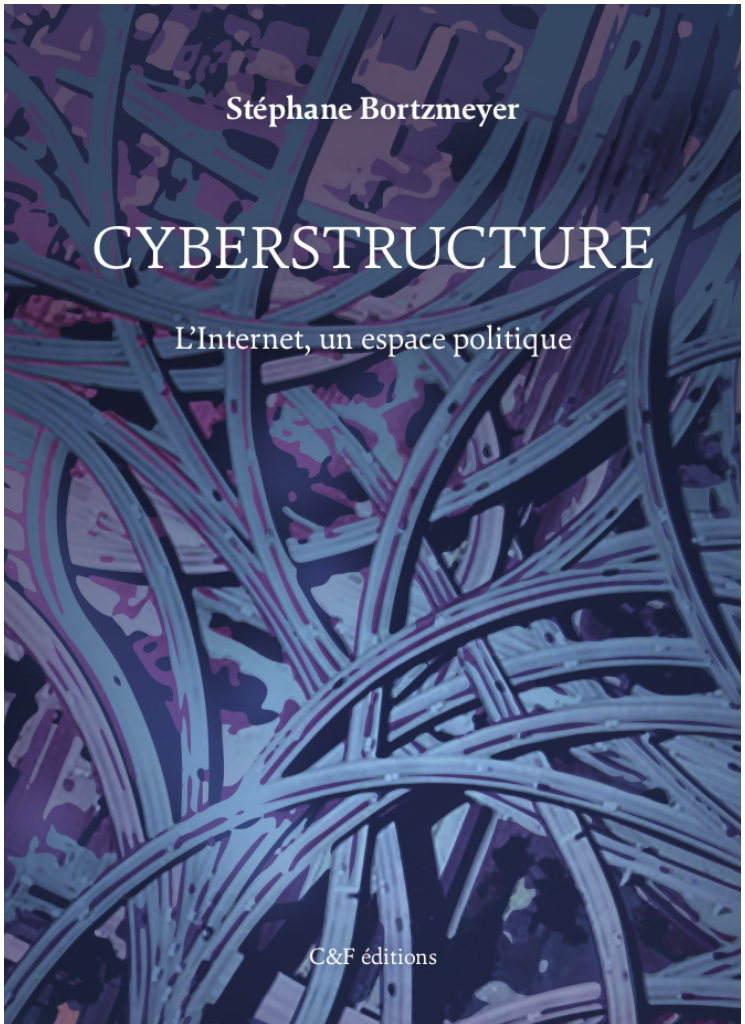
Cyberstructure - et son rôle dans la sécurité

Stéphane Bortzmeyer
stephane+rssia@bortzmeyer.org

Assises régionales de la cyber-sécurité - RSSIA, 23 septembre 2019

Le livre

« Cyberstructure ; Internet, un espace politique », chez C&F Éditions `https://cyberstructure.fr/`



De quoi ça parle

De quoi ça parle

- De l'**infrastructure** de l'Internet (tout ce qui n'est pas sur l'écran),

De quoi ça parle

- De l'**infrastructure** de l'Internet (tout ce qui n'est pas sur l'écran),
- Que tout le monde devrait connaitre un minimum,

De quoi ça parle

- De l'**infrastructure** de l'Internet (tout ce qui n'est pas sur l'écran),
- Que tout le monde devrait connaitre un minimum,
- Vu son importance dans ce qu'on peut ou ne peut pas faire (facilement) sur l'Internet.

De quoi ça parle

- De l'**infrastructure** de l'Internet (tout ce qui n'est pas sur l'écran),
- Que tout le monde devrait connaitre un minimum,
- Vu son importance dans ce qu'on peut ou ne peut pas faire (facilement) sur l'Internet.
- Technique et politique sont donc mêlés.

Car l'infrastructure compte

Car l'infrastructure compte

- « *Who should your computer take its orders from ? Most people think their computers should obey them, not obey someone else.* » (Richard Stallman)

Car l'infrastructure compte

- « *Who should your computer take its orders from ? Most people think their computers should obey them, not obey someone else.* » (Richard Stallman)
- Vu son importance dans ce qu'on peut ou ne peut pas faire (facilement) sur l'Internet.

La sécurité est politique

La sécurité est politique

- « La sécurité est toujours un compromis » (Bruce Schneier). Si on ne pensait qu'à la sécurité, on ne ferait pas d'informatique du tout.

La sécurité est politique

- « La sécurité est toujours un compromis » (Bruce Schneier).
- Pas seulement compromis entre sécurité et, par exemple, liberté. Mais aussi entre services de sécurité.

La sécurité est politique

- « La sécurité est toujours un compromis » (Bruce Schneier).
- Pas seulement compromis entre sécurité et, par exemple, liberté. Mais aussi entre services de sécurité.
- Attention, « il faut faire des compromis » est souvent utilisé pour nous faire avaler des couleuvres.

La sécurité est politique

- « La sécurité est toujours un compromis » (Bruce Schneier).
- Pas seulement compromis entre sécurité et, par exemple, liberté. Mais aussi entre services de sécurité.
- Attention, « il faut faire des compromis » est souvent utilisé pour nous faire avaler des couleuvres.
- La politique, c'est quand il faut faire des choix, et que tout le monde n'est pas d'accord.

La sécurité est politique

- « La sécurité est toujours un compromis » (Bruce Schneier).
- Pas seulement compromis entre sécurité et, par exemple, liberté. Mais aussi entre services de sécurité.
- Attention, « il faut faire des compromis » est souvent utilisé pour nous faire avaler des couleuvres.
- La politique, c'est quand il faut faire des choix, et que tout le monde n'est pas d'accord.
- Quelques cas concrets.

Protection contre les dDoS

Protection contre les dDoS

- Si on a un site Web très visible, on risque des attaques par déni de service,

Protection contre les dDoS

- Si on a un site Web très visible, on risque des attaques par déni de service,
- Contre la plupart des DoS, la taille compte,

Protection contre les dDoS

- Si on a un site Web très visible, on risque des attaques par déni de service,
- Contre la plupart des DoS, la taille compte,
- La solution courante est d'acheter une protection à une entreprise spécialisée, qui fera la « cyberguerre » à votre place,

Protection contre les dDoS

- Si on a un site Web très visible, on risque des attaques par déni de service,
- Contre la plupart des DoS, la taille compte,
- La solution courante est d'acheter une protection à une entreprise spécialisée, qui fera la « cyberguerre » à votre place,
- C'est un peu féodal : le seigneur protège les paysans, les paysans obéissent au seigneur.

Résolveurs DNS menteurs pour vous protéger

Résolveurs DNS menteurs pour vous protéger

- Petit rappel DNS : quasiment toute activité commence par une requête DNS, c'est donc un point de contrôle tentant,

Résolveurs DNS menteurs pour vous protéger

- Petit rappel DNS : quasiment toute activité commence par une requête DNS, c'est donc un point de contrôle tentant,
- *DNS firewall*, *Umbrella* et autres noms gentils,

Résolveurs DNS menteurs pour vous protéger

- Petit rappel DNS : quasiment toute activité commence par une requête DNS, c'est donc un point de contrôle tentant,
- *DNS firewall*, *Umbrella* et autres noms gentils,
- Qui décide de ce qui est malveillant ?

Résolveurs DNS menteurs pour vous protéger

- Petit rappel DNS : quasiment toute activité commence par une requête DNS, c'est donc un point de contrôle tentant,
- *DNS firewall*, *Umbrella* et autres noms gentils,
- Qui décide de ce qui est malveillant ?
- Qui l'installe ? L'utilisateur (Pi-Hole, Turris Omnia avec liste de blocage) ?

DoH (DNS-over-HTTPS)

DoH (DNS-over-HTTPS)

- Les FAI se permettent de modifier requêtes et réponses DNS en route, ou bien d'avoir des résolveurs menteurs,

DoH (DNS-over-HTTPS)

- Les FAI se permettent de modifier requêtes et réponses DNS en route, ou bien d'avoir des résolveurs menteurs,
- DoT (DNS-over-TLS) et DoH permettent de communiquer de manière sûre avec un résolveur distant, comme `https://doh.bortzmeyer.fr/` et `dot.bortzmeyer.fr`,

DoH (DNS-over-HTTPS)

- Les FAI se permettent de modifier requêtes et réponses DNS en route, ou bien d'avoir des résolveurs menteurs,
- DoT (DNS-over-TLS) et DoH permettent de communiquer de manière sûre avec un résolveur distant,
- Ce qui ne plait pas à tout le monde (cf. annonce de Mozilla le 6 septembre),

DoH (DNS-over-HTTPS)

- Les FAI se permettent de modifier requêtes et réponses DNS en route, ou bien d'avoir des résolveurs menteurs,
- DoT (DNS-over-TLS) et DoH permettent de communiquer de manière sûre avec un résolveur distant,
- Ce qui ne plait pas à tout le monde,
- Plein de questions politiques : pouvoir au FAI ou bien au navigateur ? Quel choix pour l'utilisateur, et comment lui présenter ?

BGP et le routage

BGP et le routage

- Par défaut, un routeur BGP accepte les annonces des autres routeurs sans discuter,

BGP et le routage

- Par défaut, un routeur BGP accepte les annonces des autres routeurs sans discuter,
- Petit à petit, des moyens de vérifier les annonces sont apparus (signatures avec la RPKI),

BGP et le routage

- Par défaut, un routeur BGP accepte les annonces des autres routeurs sans discuter,
- Petit à petit, des moyens de vérifier les annonces sont apparus,
- Mais ne sont pas toujours déployés.

BGP et le routage

- Par défaut, un routeur BGP accepte les annonces des autres routeurs sans discuter,
- Petit à petit, des moyens de vérifier les annonces sont apparus,
- Mais ne sont pas toujours déployés.
- La grande majorité des signatures sont déléguées au RIPE. Est-ce un progrès ?

Pas touche à mon infra

Pas touche à mon infra

- Déclaration de l'IAB (*Internet Architecture Board*) le 4 septembre,

Pas touche à mon infra

- Déclaration de l'IAB le 4 septembre,
- Sanctuariser l'infrastructure de l'Internet ?

Pas touche à mon infra

- Déclaration de l'IAB le 4 septembre,
- Sanctuariser l'infrastructure de l'Internet ?
- Censure et contrôle dans les extrémités ?

Pare-feux

Pare-feux

- Sans pare-feu, l'Internet est dangereux,

Pare-feux

- Sans pare-feu, l'Internet est dangereux,
- Mais qui décide de ce qu'il bloque ? (Services, serveurs.)

Le navigateur veut votre bien

Le navigateur veut votre bien

- « Ce site est dangereux, Chrome/Firefox/Edge ne vous laisse pas y accéder. »

Le navigateur veut votre bien

- « Ce site est dangereux, Chrome/Firefox/Edge ne vous laisse pas y accéder. »
- Mon Wordpress est piraté, mis sur une liste noire, les navigateurs décident de le bloquer.

Le navigateur veut votre bien

- « Ce site est dangereux, Chrome/Firefox/Edge ne vous laisse pas y accéder. »
- Mon Wordpress est piraté, mis sur une liste noire, les navigateurs décident de le bloquer.
- Bloquer tel ou tel site dans les logiciels clients ?

Magasins d'applications

Magasins d'applications

- Vieille idée du logiciel libre (Debian),

Magasins d'applications

- Vieille idée du logiciel libre (Debian),
- Reprise par Apple pour l'App Store et Google pour Play,

Magasins d'applications

- Vieille idée du logiciel libre (Debian),
- Reprise par Apple pour l'App Store et Google pour Play,
- Qui décide de ce qu'on peut y mettre ?

Magasins d'applications

- Vieille idée du logiciel libre (Debian),
- Reprise par Apple pour l'App Store et Google pour Play,
- Qui décide de ce qu'on peut y mettre ?
- Un audit de sécurité par application ?

Magasins d'applications

- Vieille idée du logiciel libre (Debian),
- Reprise par Apple pour l'App Store et Google pour Play,
- Qui décide de ce qu'on peut y mettre ?
- Un audit de sécurité par application ?
- Signal et F-Droid.