

News for nerds, stuff that matters

- [Login](#)
- [Create Account](#)
- [Subscribe](#)

- [Why Login?](#)
- [Why Subscribe?](#)

Log in

Nickname

Password

Public Terminal

Log in

[[Create a new account](#)]

Opinion Center: [Intel](#)

EU To Counter Echelon With Quantum Cryptography?

Posted by [simoniker](#) on Mon May 17, '04 06:17 PM
from the if-it-exists dept.

jfruhlinger writes "An article on Security.ITWorld.com seems to [outline a coming information arms race](#). The European Union has decided to respond to the [Echelon project](#) by funding research into supposedly unbreakable quantum cryptography that will keep EU data out of Echelon's maw. Leaving aside the question of whether such a thing is possible, the political implications are troubling, indicating a widening rift within the Western world. Interestingly, the UK is part of the EU, but its intelligence services are among Echelon's sponsors."



- **What I do is....**

(Score:5, Funny)

by [Kenja \(541830\)](#) on Monday May 17, @06:19PM ([#9177834](#))
(<http://www.netweasel.com/>)

What I do is send meaningless emails with high encryption to my friends in China. I figure that the NSA may as well spend countless CPU cycles finding out that I just installed the Guild Wars E3 demo rather than on important stuff.

- [Re:What I do is....](#) by Anonymous Coward (Score:1) Monday May 17, @06:30PM
- **Re:What I do is....**

(Score:5, Funny)

by [DynaSoar \(714234\)](#) * on Monday May 17, @06:39PM ([#9178041](#))
(Last Journal: [Sunday June 19, @02:43PM](#))

"What I do is send meaningless emails with high encryption to my friends in China. I figure that the NSA may as well spend countless CPU cycles finding out that I just installed the Guild Wars E3 demo rather than on important stuff."

I often enjoy sending such things are core dumps or font files (or maybe plans for a planet-buster nuke, I fergit) compressed twice using two different out dated compression programs (say, ARC on a PC and then ShrinkIt [NuFX] on an Apple II), strip off the archive ID header, UUencode it, strip off the leading cap M's, cut it in half, paste it second half first into an email, and send it with a subject line with likely Echelon trigger words, adding "PS: Call me for the key to decode this." If encryption is outlawed, only

a8e3 5m0w s3k1 5d9k

b7f2 7k1l c9r4 3yr5.

[[Parent](#)]

- [Re:What I do is....](#) by SmackCrackandPot (Score:3) Monday May 17, @07:03PM
- [Re:What I do is....](#) by pracz (Score:3) Monday May 17, @07:48PM

- [Re:What I do is....](#) by igny (Score:1) Tuesday May 18, @07:41AM
 - [Re:What I do is....](#) by thrillseeker (Score:3) Monday May 17, @10:11PM
 - [Re:What I do is....](#) by h4rm0ny (Score:2) Tuesday May 18, @06:41AM
 - [Surely they would notice](#) by eldacan (Score:1) Tuesday May 18, @07:00AM
- **Re:What I do is....**

(Score:5, Funny)

by [Mazzaroth \(519229\)](#) on Monday May 17, @10:04PM ([#9179541](#))
(<http://www.edouardboily.com/>)

I remember using that kind of tactic back then... I was in charge of a research group and we had to produce a huge specification document for friday 17h00. Of course it was not ready on time. So I decided to try something. I first included a few copies of the document (10 or so) in a zip archive, I then encrypted it using PGP, then uuencoded it, performed a shuffling on it and finally zipped-it again and re-PGP it. After removing the heading, I renamed the thing "Spec_1.0.doc" and send it to our customer. Of course we worked all weekend completing the document but at least, it registered, as our contract required, just in time. The customer came back to us one week later saying that they were not able to open the MSWord document. "Oh! (we said), gee! This must be this email thing AGAIN... we've been having this problem lately... let me resend it to you". And I sent the (new, completed and heavily revised) document. The customer were happy because the document were very good, and so were we.

I think this time-dilatation technique has been called 'Ed's relativistic document delivery' in that company I used to work. I just called it 'creativity by necessity'.

[[Parent](#)]

- [Re:What I do is....](#) by bfg9000 (Score:2) Tuesday May 18, @10:32AM
 - [Re:What I do is....](#) by DynaSoar (Score:2) Tuesday May 18, @01:27PM
- [Re:What I do is....](#) by Giant Panda (Score:1) Monday May 17, @07:01PM
- [Re:What I do is....](#) by nemesisj (Score:3) Tuesday May 18, @12:39AM
- [Re:What I do is....](#) by MoonBuggy (Score:2) Monday May 17, @06:34PM
- [Re:What I do is....](#) by ScottGant (Score:2) Monday May 17, @06:44PM
 - [Re:What I do is....](#) by JamesKPolk (Score:1) Monday May 17, @06:47PM
 - [Re:What I do is....](#) by arcanumas (Score:2) Monday May 17, @07:03PM
 - [Re:What I do is....](#) by arcanumas (Score:2) Monday May 17, @06:51PM
 - [Re:What I do is....](#) by Detritus (Score:2) Monday May 17, @08:16PM
- [Re:What I do is....](#) by aurelian (Score:3) Monday May 17, @06:45PM
 - [Re:What I do is....](#) by d474 (Score:1) Tuesday May 18, @01:29AM
 - [Re:What I do is....](#) by cicho (Score:2) Tuesday May 18, @08:29AM
- [I've heard...](#) by Anonymous Coward (Score:1) Monday May 17, @07:47PM
 - [Re:I've heard...](#) by sfjoe (Score:2) Monday May 17, @10:10PM
 - [Re:I've heard...](#) by packeteer (Score:2) Monday May 17, @11:02PM
 - **Re:I've heard...**

(Score:4, Insightful)

by [ComaVN \(325750\)](#) on Tuesday May 18, @03:00AM ([#9180874](#))

You assume catching "regular" criminals is high-priority for the government, which it probably isn't. IF they can break it, it would be far more valuable to use it for military purposes and against terrorists, and keeping it a secret is worth more than catching some random mobster.

Catching a terrorist, or "unlawful combatant" or whatever the mot-du-jour is, using this technology, will NOT become common knowledge, since it's not like terrorists get anything resembling a fair and open trial on their island resort in the caribbean, is it?

Not that I think they can break it quite that fast, at least not in bulk.

[[Parent](#)]

- [Re:I've heard...](#) by StillNeedMoreCoffee (Score:3) Tuesday May 18, @10:45AM
 - [Re:I've heard...](#) by Cili (Score:1) Wednesday May 19, @04:31AM
 - [Re:I've heard...](#) by StillNeedMoreCoffee (Score:2) Thursday May 20, @12:13PM
 - [Re:I've heard...](#) by seafoodforklift (Score:2) Tuesday May 18, @04:58AM

- [Re:What I do is....](#) by some guy I know (Score:1) Tuesday May 18, @02:31AM
- [Re:It is better to stop the government corruption.](#) by niiler (Score:1) Tuesday May 18, @09:32AM
- [Re:What I do is....](#) by shamino0 (Score:2) Wednesday May 19, @03:52PM
- **6 replies beneath your current threshold.**
- [ummm...](#) by Anonymous Coward (Score:2) Monday May 17, @06:20PM
 - [Re:ummm...](#) by treerex (Score:1) Monday May 17, @06:27PM
 - [More](#) by Anonymous Coward (Score:1) Monday May 17, @06:53PM
 - **Re:ummm...**

(Score:5, Informative)

by Anonymous Coward on Monday May 17, @06:32PM ([#9177951](#))

Sigh.. OK, it's a troll, but someone has to bite.

a. Quantum crypto is invulnerable to a monkey-in-the-middle attack. Poorly implemented SSL is vulnerable to MITM during key exchange.

2. It is widely accepted lore on the Internet, and strongly suspected by respectable people, that there exist quantum computing devices capable of factoring extremely large numbers. If this is true, any form of public-key crypto goes to shit.

iii. Part of the problem with cryptography is that it does nothing to hide the source and destination of the data exchange. In theory, a secure quantum crypto system can't be tapped in the first place, so in theory, sender and receiver are anonymous.

IV. H.323 is for godless commies.

[[Parent](#)]

- **Re:ummm...**

(Score:5, Informative)

by [MonMotha \(514624\)](#) on Monday May 17, @08:04PM ([#9178802](#))

Remember, there are two major systems for doing public key crypto. The idea is to take a problem that is incredibly easy to do one way (make the public key from the private), but very difficult to do the reverse of. Factoring large numbers is a great example (and is what RSA uses). It's easy to multiply two large primes, but much more difficult to factor the product back into the original two primes. If there were a computer which could do this quickly, RSA would be effectively useless.

There is also the discrete log problem, which is what DSA uses. I don't pretend to be a cryptographer, or even know really what the discrete log problem involves (no google links please, I have all the info I need on it if I were really interested), but I do know that it is very easy to do one way, but very hard to do the other! Exactly what you need for public key crypto. Now, if we have a theoretical computer which can break this in reasonable time, DSA becomes worthless. However, there are definitely other ways of doing public key crypto than the factoring problem.

Also, another interesting thing about quantum crypto (of course, quantum crypto is largely theoretical at this point, so this is not guaranteed in real world implementations) is that both ends KNOW if the datastream has been intercepted. Not just if it's been modified (we can be reasonably sure of that right now using good hashing algorithms for signatures), but if it has nearly been intercepted. This is quite handy because now you know immediately if you need to somehow change things since your data is even POSSIBLY compromised. Really cool stuff.

I must reiterate, IANAC (cryptographer).

[[Parent](#)]

- [Re:ummm...](#) by arevos (Score:2) Tuesday May 18, @09:35AM
- [Re:ummm...](#) by pracz (Score:1) Monday May 17, @08:06PM
- **2 replies beneath your current threshold.**
- **Uh oh...**

(Score:4, Funny)

by [ryanvm \(247662\)](#) on Monday May 17, @06:21PM (#9177845)

The Whitehouse just issued a press release stating that, "Quantum Mechanics is now officially part of the Axis of Evil".

- o **Re:Uh oh...**

(Score:5, Funny)

by [theefer \(467185\)](#) * on Monday May 17, @06:33PM (#9177962)

(<http://www.milcis.net/>)

If you don't consider Quantum Physics evil, you've definitely never been in a technical university.

[[Parent](#)]

- [Re:Uh oh...](#) by Dr.Knackerator (Score:1) Tuesday May 18, @03:50AM
- o [Re:Uh oh...](#) by sandbagger (Score:1) Monday May 17, @07:29PM
 - **1 reply beneath your current threshold.**
- o **Re:Uh oh...**

(Score:4, Funny)

by [brain159 \(113897\)](#) on Monday May 17, @07:44PM (#9178647)

(<http://analogypolice.com/> | Last Journal: [Thursday January 09, @09:28PM](#))

Surely, quantum mechanics might or might not be part of the axis of evil?

[[Parent](#)]

- [Re:Uh oh...](#) by igny (Score:1) Tuesday May 18, @07:21AM
 - **1 reply beneath your current threshold.**
 - o [Re:Uh oh...](#) by erik_norgaard (Score:1) Tuesday May 18, @07:14AM
 - o **2 replies beneath your current threshold.**
- **Unbeatable Encryption!**

(Score:5, Funny)

by Anonymous Coward on Monday May 17, @06:21PM (#9177847)

In other news, a significant minority of people in the EU have already switched to an unbreakable real-time encryption technology, transmissible through the open air. External experts are at a loss; the NSA has made no headway whatsoever against this new threat.

What is it? It goes by the name 'French'...

- o **Re:Unbeatable Encryption!**

(Score:5, Interesting)

by [cjellibebi \(645568\)](#) on Monday May 17, @06:31PM (#9177947)

Speaking of which, didn't the US government during WWII translate some of their top-secret documents into one of the languages of the Native Americans? I think they chose that particular language because it had unique properties that made de-cyphering the language almost impossible. I'm not sure if they applied any additional encryption, or what would have happened if the enemy had somehow managed to kidnap a speaker of that language.

Is this just 'security through obscurity', or was there something else involved.

[[Parent](#)]

- **Re:Unbeatable Encryption!**

(Score:5, Informative)

by [nacturation \(646836\)](#) on Monday May 17, @06:36PM (#9178009)

(Last Journal: [Thursday May 25, @01:44AM](#))

You're thinking of [Navajo code](#) [google.com]. Should be enough to keep you busy reading for a while.

.)

[[Parent](#)]

- **1 reply beneath your current threshold.**
- [Re:Unbeatable Encryption!](#) by nkh (Score:1) Monday May 17, @06:40PM

■ **Re:Unbeatable Encryption!**

(Score:5, Informative)

by [SirWhoopass \(108232\)](#) on Monday May 17, @06:42PM ([#9178076](#))

The US Marine Corps enlisted members of the [Navajo tribe](#) [navy.mil] to act as radio operators in the Pacific. The language had never been written, and it was estimated there were fewer than 30 non-native speakers at the outbreak of World War II.

Earlier, in World War I, the US Army utilized [members of the Choctaw tribe](#) [essortment.com] as operators near the end of the war. This, however, was due to a decision in the field (a captain noted that he had several members of the tribe in his battalion), rather than a formal program.

[[Parent](#)]

■ **Re:Unbeatable Encryption!**

(Score:5, Informative)

by [Shakrai \(717556\)](#) on Monday May 17, @06:44PM ([#9178089](#))

(Last Journal: [Friday December 09, @07:03PM](#))

I think they chose that particular language because it had unique properties that made de-cyphering the language almost impossible. I'm not sure if they applied any additional encryption

The [Navajo Code Talkers](#) [navy.mil]. They didn't apply additional encryption per say but they had an interesting encoding scheme:

When a Navajo code talker received a message, what he heard was a string of seemingly unrelated Navajo words. The code talker first had to translate each Navajo word into its English equivalent. Then he used only the first letter of the English equivalent in spelling an English word. Thus, the Navajo words "wol-la-chee" (ant), "be-la-sana" (apple) and "tse-nill" (axe) all stood for the letter "a." One way to say the word "Navy" in Navajo code would be "tsah (needle) wol-la-chee (ant) ah-keh-di- glini (victor) tsah-ah-dzoh (yucca)."

Most letters had more than one Navajo word representing them. Not all words had to be spelled out letter by letter. The developers of the original code assigned Navajo words to represent about 450 frequently used military terms that did not exist in the Navajo language. Several examples: "besh- lo" (iron fish) meant "submarine," "dah-he- tih-hi" (hummingbird) meant "fighter plane" and "debeh-li-zine" (black street) meant "squad."

You can also assume that they encoded the messages using standard military/common-sense methods -- i.e: referring to waypoints on a map that your enemy doesn't have access to. If he knows that you are going to attack at "Point Echo" but he doesn't know where that is the information is of limited use to him -- by the time he figures out where Point Echo is the information is out of date and it doesn't matter that he knows it.

In any case the code talkers are an interesting (often ignored) fact of WW2, the [recent movie](#) [imdb.com] notwithstanding. An interesting subject to read up on sometime.

[[Parent](#)]

- [Re:Unbeatable Encryption!](#) by cxvx (Score:2) Monday May 17, @06:45PM
- [Re:Unbeatable Encryption!](#) by rgriff59 (Score:1) Monday May 17, @06:50PM
 - **1 reply beneath your current threshold.**
- **Re:Unbeatable Encryption!**

(Score:5, Informative)

by [chadjg \(615827\)](#) <chadgessele2000.yahoo@com> on Monday May 17, @07:37PM ([#9178581](#))

(Last Journal: [Friday February 13, @02:08PM](#))

If I remember the story correctly, Navajo demands very precise pronunciation and accents. getting the

nuances just right is supposed to be next to impossible right for a non-native speaker.

So, even if a few Japanese operators did learn Navajo, they wouldn't be able to spoof their way onto the network. Kinda like trying to read the state of a photon without blowing the secret, maybe.

Throw in the fact that the Japanese probably didn't care at all about the various tribes, even if they did know what a Navajo was, and you have a tough nut to crack. The war didn't last long enough for them to adapt.

I remember watching some TV special about the code talkers, and one of the old guys was practically laughing when he was telling his story. Good stuff.

[[Parent](#)]

■ **Re:Unbeatable Encryption!**

(Score:5, Funny)

by [pipingguy \(566974\)](#) on Monday May 17, @10:21PM (#9179624)

(<http://www.pipingdesign.com/>)

I remember watching some TV special about the code talkers, and one of the old guys was practically laughing when he was telling his story.

When NASA was preparing for the Apollo project, they did some astronaut training on a Navajo Indian reservation. One day, a Navajo elder and his son were herding sheep and came across the space crew. The old man, who spoke only Navajo, asked a question which his son translated. "What are these guys in the big suits doing?"

A member of the crew said they were practicing for their trip to the moon. The old man got all excited and asked if he could send a message to the moon with the astronauts.

Recognizing a promotional opportunity for the spin-doctors, the NASA folks found a tape recorder. After the old man recorded his message, they asked the son to translate it. He refused.

So the NASA reps brought the tape to the reservation where the rest of the tribe listened and laughed but refused to translate the elder's message to the moon.

Finally, the NASA crew called in an official government translator. He reported that the moon message said, "Watch out for these guys; they have come to steal your land."

[[Parent](#)]

■ [Re:Unbeatable Encryption! - Navajo Joke](#) by Anonymous Coward (Score:1) Tuesday May 18, @11:51AM

■ **1 reply beneath your current threshold.**

■ [Re:Unbeatable Encryption!](#) by esampson (Score:2) Monday May 17, @08:04PM

■ [Re:Unbeatable Encryption!](#) by Rick.C (Score:2) Tuesday May 18, @08:34AM

○ **1 reply beneath your current threshold.**

● [Measures and counter-measures](#) by TheDarkener (Score:2) Monday May 17, @06:22PM

○ [Re:Measures and counter-measures](#) by rokzy (Score:3) Monday May 17, @06:27PM

■ [Re:Measures and counter-measures](#) by Kirill Lokshin (Score:3) Monday May 17, @06:40PM

■ [Re:Measures and counter-measures](#) by Jerf (Score:3) Monday May 17, @06:56PM

■ [Re:Measures and counter-measures](#) by Kirill Lokshin (Score:2) Monday May 17, @07:05PM

■ [Re:Measures and counter-measures](#) by Karhath (Score:2) Monday May 17, @07:36PM

■ [Re:Measures and counter-measures](#) by d474 (Score:2) Tuesday May 18, @01:47AM

○ [Re:Measures and counter-measures](#) by TheRaven64 (Score:2) Monday May 17, @06:32PM

○ [Re:Measures and counter-measures](#) by ClausCCC (Score:3) Monday May 17, @06:37PM

■ [Re:Measures and counter-measures](#) by servognome (Score:1) Monday May 17, @07:11PM

■ [Re:Measures and counter-measures](#) by Karhath (Score:2) Monday May 17, @07:32PM

■ [Re:Measures and counter-measures](#) by servognome (Score:1) Monday May 17, @09:41PM

■ [Re:Measures and counter-measures](#) by drig (Score:2) Monday May 17, @11:41PM

■ **1 reply beneath your current threshold.**

○ [Re:Measures and counter-measures](#) by CanadianCrackPot (Score:1) Tuesday May 18, @06:59AM

● **The interesting case of the UK**

(Score:5, Insightful)

by [Rosco P. Coltrane \(209368\)](#) on Monday May 17, @06:22PM ([#9177861](#))

Interestingly, the UK is part of the EU, but its intelligence services are among Echelon's sponsors.

The UK has its butt sitting on 2 chairs. On one hand they sort of behave like a US state, with Tony as governor, and on the other as a half-willing EU member, in large part thanks to Mrs Thatcher. One of these days they'll have to decide which continent they want to be part of.

And I have a feeling that, if the population has a say, they'll embrace the EU eventually. Of course, the population rarely has a true say in any country though...

○ **Re:The interesting case of the UK**

(Score:5, Insightful)

by [JamesKPolk \(13313\)](#) on Monday May 17, @06:27PM ([#9177906](#))

(<http://www.hakubi.us/>)

The British population would like to be able to develop close ties without giving up their own national sovereignty. Whether the EU allows that will determine how close the UK gets to the rest of western Europe.

[[Parent](#)]

■ **Re:The interesting case of the UK**

(Score:5, Interesting)

by [nickos \(91443\)](#) on Monday May 17, @06:33PM ([#9177964](#))

I'm a pro-European, but we have to make the EU more democratic. The fact is that the members of the EU have already given up large amounts of their national sovereignty (because EU members must implement EU directives). This in itself is not necessarily a bad thing, as long as EU law is created by democratically elected representatives at the European supra-national level.

[[Parent](#)]

■ **Re:The interesting case of the UK**

(Score:5, Insightful)

by [jsebrech \(525647\)](#) on Monday May 17, @07:43PM ([#9178636](#))

There is a EU parliament with democratically elected representatives. The problem is that the council, which isn't elected, can overrule it on a lot of issues. Like how the council reverted the software patent draft to a version that seems written by a microsoft lawyer, despite an explicit voting record in parliament that goes directly against that.

[[Parent](#)]

■ [Re:The interesting case of the UK](#) by DiscoDave_25 (Score:2) Tuesday May 18, @06:33AM

■ [Re:The interesting case of the UK](#) by hawkfish (Score:2) Tuesday May 18, @06:46PM

■ [Re:The interesting case of the UK](#) by jsebrech (Score:3) Tuesday May 18, @07:26AM

■ **1 reply beneath your current threshold.**

■ [Re:The interesting case of the UK](#) by cjllibebi (Score:3) Monday May 17, @06:39PM

■ [Re:The interesting case of the UK](#) by 91degrees (Score:1) Monday May 17, @06:51PM

■ [Re:The interesting case of the UK](#) by cjllibebi (Score:2) Monday May 17, @07:11PM

■ **Re:The interesting case of the UK**

(Score:4, Insightful)

by [Space cowboy \(13680\) *](#) on Monday May 17, @06:55PM ([#9178204](#))

(Last Journal: [Monday April 17, @02:39PM](#))

And yet you look at the employment rates within the UK and the rest of Europe (3% vs 12% approx) The UK is hardly a panacea but if you're willing to go for a lower paid job than you think you deserve, you'll prosper. It's always easier to get another job when you already have a

job....

Personally given the fact that the UK is the driving force behind software patents in the EU, I will be voting against the government and against anything EU-centric in the upcoming elections. I don't see that it's at all democratic for the EU parliament (I think) to decide amendments need to be made, then the EU Council of ministers to ride roughshod over the whole thing. Go Germany, I wish the UK government had half the cluebat you wield....

I wonder if the UK gets a net gain from being in Europe, I really do. Consider if we *did* become the 51st state. The real problem would be that the US people would never accept it - we have 56 million people, the US has 260 million. If the UK became a state, it would represent 1/6 the population of the USA, never mind the influence the commonwealth brings in... The Whitehouse would have to be relocated to 10 Downing St. Can't see it myself... Empire by default - never happen, given our history...

Simon

[[Parent](#)]

- [Re:The interesting case of the UK](#) by antiMStroll (Score:3) Monday May 17, @07:39PM
 - [Re:The interesting case of the UK](#) by pommiekiwifruit (Score:1) Monday May 17, @09:48PM
- [Re:The interesting case of the UK](#) by AndrewHowe (Score:1) Monday May 17, @07:52PM
- [Re:The interesting case of the UK](#) by Tiro (Score:2) Monday May 17, @09:01PM
 - **1 reply beneath your current threshold.**
- [Re:The interesting case of the UK](#) by bishop32x (Score:1) Monday May 17, @09:21PM
- [Re:The interesting case of the UK](#) by pantycrickets (Score:2) Monday May 17, @10:28PM
- [Parent has woefully wrong numbers - link](#) by Anonymous Coward (Score:2) Monday May 17, @11:01PM
- **Re:The interesting case of the UK**

(Score:5, Informative)

by [Malc \(1751\)](#) on Tuesday May 18, @12:33AM ([#9180372](#))

"And yet you look at the employment rates within the UK and the rest of Europe (3% vs 12% approx)"

Where did you get those numbers? According to this week's Economist, the rate is 4.7% in Britain and 8.8% in the Euro area. The UK rate is still extremely low, but not as exaggerated as you stated.

[[Parent](#)]

- [Re:The interesting case of the UK](#) by miu (Score:2) Tuesday May 18, @03:54AM
 - [Re:The interesting case of the UK](#) by The Lynxpro (Score:2) Tuesday May 18, @12:57PM
 - [Re:The interesting case of the UK](#) by miu (Score:2) Tuesday May 18, @05:56PM
 - [Re:The interesting case of the UK](#) by SkunkPussy (Score:1) Tuesday May 18, @07:21PM
 - **1 reply beneath your current threshold.**
- [Re:The interesting case of the UK](#) by Mant (Score:2) Tuesday May 18, @05:46AM
 - [Re:The interesting case of the UK](#) by The Lynxpro (Score:2) Tuesday May 18, @01:35PM
- [it is conomic earning power not population](#) by Archfeld (Score:2) Friday May 21, @03:53PM
 - [Re:The interesting case of the UK](#) by VdG (Score:1) Tuesday May 18, @07:07AM
- [Re:The interesting case of the UK](#) by JamesKPolk (Score:1) Monday May 17, @06:55PM
 - [Re:The interesting case of the UK](#) by treworkan (Score:1) Monday May 17, @08:15PM
 - [Re:The interesting case of the UK](#) by lonesome phreak (Score:2) Tuesday May 18, @12:21AM
 - **1 reply beneath your current threshold.**
 - **2 replies beneath your current threshold.**

o **Re:The interesting case of the UK**

(Score:4, Interesting)

by [patrick_jones \(95543\)](#) * <<[azurlune](#)> <at> <[gmail.com](#)>> on Monday May 17, @06:34PM ([#9177987](#)) (<http://www.the-dot.org/>)

I have a feeling, if the population get a say, we will be out of Europe completely, the gates of the country will be shut, and the key thrown away. The British public is controlled by the gutter press (Mail, Times, Express, Sun) who are all vehemently Euro-sceptic. Well, controlled is too strong a word, but all the stories in those papers are anti-EU, anti-immigrant, anti-everything except good ole British values, like taking over half of the world.

And calling Britian the 51st state is just wrong. For a start, most of us object to the US, and so do most of the Foreign Office. The sympathy to the US is due to long standing ties, like us running you, and the fact we speak the same language. We try and imagine ourself as a bridge between the two continents. Not that that really works...

[[Parent](#)]

- [Re:The interesting case of the UK](#) by caitsith01 (Score:3) Monday May 17, @08:32PM

o **Re:The interesting case of the UK**

(Score:4, Informative)

by [ShadeARG \(306487\)](#) on Monday May 17, @06:42PM ([#9178070](#))

Wikipedia has some interesting information on [ECHELON](#) [wikipedia.org] .

[[Parent](#)]

o **Half-willing?**

(Score:5, Interesting)

by [pjt33 \(739471\)](#) on Monday May 17, @06:47PM ([#9178122](#))

(<http://pjt33.f2g.net/>)

Tony wants to be at the centre of the EU, and so do the Lib Dems. I've no idea what the official Tory line is this week, nor how many of them support it, but there's a very solid majority in the House of Commons pushing a pro-EU agenda.

[[Parent](#)]

- [Re:Half-willing?](#) by Cally (Score:2) Tuesday May 18, @06:57AM
- [Re:Half-willing?](#) by term8or (Score:1) Tuesday May 18, @08:15AM
- [Mod parent up as Funny](#) by pjt33 (Score:2) Tuesday May 18, @10:11AM
- **1 reply beneath your current threshold.**

o **Thatcher wasn't pro Europe**

(Score:5, Informative)

by [T-Kir \(597145\)](#) on Monday May 17, @07:19PM ([#9178440](#))

(<http://slashdot.org/~T-Kir>)

Mrs Thatcher was distinctly anti-Euro, apart from free trade and good relations which follows the last referendum the UK had. It was the Major years (Maastricht treaty and in then out of the ERM) followed by Blair who pursued the closer ties.

Despite being promised a referendum on the EU constitution (which is a woeful hack of previous revisions), the British public hasn't been given a date on it... and the trust (read as 'lack of') I have in Blair is as such that he would do the referendum after the point of no return (sorry people if you voted 'no', it's too late now!).

I for one would like the closer ties with Europe (i.e. what we have now), but what is proposed I think is too much too soon... and there are too many problems which really need sorting first (red tape, beaurocracy, politicians voting in new laws when they have no clue as to what they are, etc etc). Added to that the majority of the British public need to know exactly what is going on, and what will happen before we're even semi happy with it.

I've always been of liberal views and what you would call a floating voter, but I wouldn't trust the Lib Dems (almost wanting to powershare with Labour, no real manifesto), I definately don't trust Blair.... but despite his previous convictions I think the Conservatives are in a much stronger position with Howard (especially

regarding party unity).

Maybe the biggest problem that'll hit us in a couple of years is the national debt (where the conservatives saved a crap load of money by taxing the country half to death - mind Labour were happy to add to that) and the housing prices/issues, add to that the amount of money being literally thrown at the NHS is a nice little ticking time bomb that I'm not looking forward to going off.

Anyway, most opinion/info in this post is AFAIK and is open to correction/counter viewpoints... as they say (damn this zippy led US keyboard), just my 0.02 UK Sterling (yes I do know about character map, I just can't be arsed!).

T-Kir

[[Parent](#)]

■ **1 reply beneath your current threshold.**

- [Re:The interesting case of the UK](#) by Alci12 (Score:1) Monday May 17, @07:57PM
- [The Logical Choice for Britain](#) by Tiro (Score:3) Monday May 17, @08:57PM
 - [Re:The Logical Choice for Britain](#) by mr_sas (Score:1) Tuesday May 18, @06:08AM
- [Re:The interesting case of the UK](#) by Threni (Score:1) Tuesday May 18, @05:41AM
 - [Re:The interesting case of the UK](#) by dappman (Score:1) Tuesday May 18, @07:24AM
- [Re:The interesting case of the UK](#) by bigsmelly (Score:1) Tuesday May 18, @05:53AM
- [Re:The interesting case of the UK](#) by sql*kitten (Score:2) Tuesday May 18, @07:52AM
- [Re:The interesting case of the UK](#) by amightywind (Score:2) Tuesday May 18, @10:19AM
- **1 reply beneath your current threshold.**
- [broad daylight](#) by Digitus1337 (Score:2) Monday May 17, @06:22PM
 - [Re:broad daylight](#) by destiney (Score:2) Monday May 17, @06:30PM
- **Quantum Encryption?**

(Score:5, Informative)

by [AKAImBatman \(238306\)](#) <akaimbatman@gmail.com minus [herbivore](#)> on Monday May 17, @06:23PM ([#9177874](#))

(<http://www.intelligentblogger.com/> | Last Journal: [Thursday May 04, @02:11PM](#))

One has to wonder why we call it Quantum Encryption when it really has nothing to do with Encryption. From the article:

The aim is to produce a communication system that cannot be intercepted by anyone

If I understand their intent, they plan to use concepts like Quantum Entanglement to ensure that communication is shared only between the entangled particles. This is a very different concept from using the properties of Quantum Mechanics to scramble information in a reversible manner or creating computers capable of super-fast calculations.

○ **Re:Quantum Encryption?**

(Score:5, Informative)

by [necama \(10131\)](#) on Monday May 17, @06:29PM ([#9177920](#))

(<http://www.auralillusion.org/>)

The point isn't to use the quantum entanglement to directly pass information back and forth; rather it is to distribute a key for a one time pad. And one time pads are provably secure, since every different one time pad gives you a different (and equally plausible) decryption of the message.

Hence, if you really want to gripe about the name, I suppose you could call it quantum key distribution.

[[Parent](#)]

- [Re:Quantum Encryption?](#) by gumbi west (Score:2) Monday May 17, @07:04PM
- [Re:Quantum Encryption?](#) by Florian Weimer (Score:3) Monday May 17, @07:06PM
 - [Re:Quantum Encryption?](#) by Karhath (Score:2) Monday May 17, @07:12PM
 - [Re:Quantum Encryption?](#) by mivok (Score:3) Monday May 17, @08:37PM
 - [Re:Quantum Encryption?](#) by addaon (Score:2) Tuesday May 18, @12:31AM

- **1 reply beneath your current threshold.**
 - [Re:Quantum Encryption?](#) by rokzy (Score:3) Monday May 17, @06:32PM
 - [Re:Quantum Encryption?](#) by Abcd1234 (Score:2) Monday May 17, @06:45PM
 - [Re:Quantum Encryption?](#) by rokzy (Score:2) Monday May 17, @06:50PM
 - [Re:Quantum Encryption?](#) by Abcd1234 (Score:2) Monday May 17, @07:01PM
 - [Re:Quantum Encryption?](#) by GileadGreene (Score:3) Monday May 17, @06:58PM
 - [Re:Quantum Encryption?](#) by rokzy (Score:2) Monday May 17, @07:06PM
 - [Re:Quantum Encryption?](#) by GileadGreene (Score:2) Monday May 17, @09:15PM

(Score:4, Insightful)

by [Karhgath \(312043\)](#) on Monday May 17, @06:33PM ([#9177965](#))
 Nope, quantum entanglement isn't used in Quantum Encryption.

As a matter of fact, you probably couldn't communicate reliably with quantum-based communication, much less quantum encryption or using quantum entanglement to communicate securely, as you hinted.

Also, I want to add a note that I personally think it shouldn't be called Quantum Encryption but "Quantum Key Distribution"(QKD), as it is a much better name for it. They use the property of quantum mechanics to exchange a key which allows them to use the one-time pad method to encrypt the message, which MUCH less logistical problems, and no way to intercept the key. The encryption algorithm is purely classical and not quantum-based. This makes QKD in such a way that it allows 2 people to communicate without anyone being able to intercept the keys with any known attacks/methods(timed, man-in-the-middle, etc.), they can only prevent them from exchanging a key and thus communicating(which in some case might be worst tho).

[[Parent](#)]

- **1 reply beneath your current threshold.**

- [Re:Quantum Encryption?](#) by javaman235 (Score:2) Monday May 17, @06:34PM
- **Quantum *Intrusion Detection***

(Score:4, Informative)

by [Jerf \(17166\)](#) on Monday May 17, @06:52PM ([#9178165](#))
<http://www.jerf.org/iri/> | Last Journal: [Saturday August 18, @12:04PM](#)

I agree. It ought to be called Quantum Intrusion Detection, because that's what it is. It doesn't encrypt, nor does it protect anybody from intercepting the message.

All it can do is tell you if your message is being intercepted. Now, this is useful information, since you might decide to quickly stop transmitting, and if you're fast enough on the draw and using conventional encryption on top of your Quantum Intrusion Detection, then you'll probably not give enough data to the intruder for them to feasibly decrypt anything.

But note that if you want the protection of encryption so the intruder doesn't get plaintext, you still need to use conventional encryption.

Also note that some wild-eyed Slashdot types who's understanding of technology is buzzword-deep sometimes make the claim that Quantum Computing might crack Quantum Encryption. Nope, because "Encryption" isn't. And the very nature of the Intrusion Detection is that you *can't* get around it, no matter how clever you are.

The worst part of this stupid naming is that some day we probably really *will* have some sort of encryption that uses QM, and then what we will call that?

Anyways, it is apparently far too late to do anything about this misnomer, but it's one of the most pernicious misnomers I've seen in modern times. Whoever named this technology should have their relevant degrees stripped.

[[Parent](#)]

- **Re:Quantum *Intrusion Detection***

(Score:5, Insightful)

by [Karhgath \(312043\)](#) on Monday May 17, @06:58PM ([#9178224](#))

Sorry to disappoint you: you are wrong. Let me explain a bit.

First, it's not Quantum Intrusion Detection. It's Quantum Key Distribution. It allows 2 people to exchange a randomly generated key as long as the message, used in a one-time pad scheme.

The trick is that the exchange of the key is unconditionally secure. Not only does it tell you when part of the key is intercepted, it also 'aborts'. The only thing an eavesdropper can do is to prevent you from communicating. If the communication is successful, then no one eavesdropped or got enough information on the key to jeopardize the exchange.

This is the beauty of it.

So no, it's not Quantum Encryption per se, as the encryption is done in classical terms using one-time pad method, but it's not Quantum Intrusion Detection either. It's a very ingenious mix of both quantum and classical methods which results in an unconditionally secure method of encryption.

And, I'd have to talk about Gilles Brassard (he teaches at the "Université de Montréal" where I study) about stripping his degrees, as he's the co-inventor of quantum encryption and computing in general. I think he'd laugh but agree that Quantum Encryption is the resulting solution, not the means. "Encryption using quantum principles" might be more revealing, but quite longer. Quantum Key Distribution is my personal favorite.

[[Parent](#)]

- [Re:Quantum *Intrusion Detection*](#) by MechaStreisand (Score:1) Monday May 17, @09:36PM
 - [Re:Quantum *Intrusion Detection*](#) by John Courtland (Score:3) Monday May 17, @10:32PM
 - [Re:Quantum *Intrusion Detection*](#) by MechaStreisand (Score:1) Tuesday May 18, @02:38AM
 - **1 reply beneath your current threshold.**
 - [Re:Quantum *Intrusion Detection*](#) by makomk (Score:1) Tuesday May 18, @05:00AM
 - **1 reply beneath your current threshold.**
- [Yes, it is encryption](#) by DrYak (Score:2) Monday May 17, @06:57PM
- [Re:Quantum Encryption?](#) by Florian Weimer (Score:2) Monday May 17, @07:04PM

• **What I find disturbing is...**

(Score:5, Insightful)

by [rokzy \(687636\)](#) on Monday May 17, @06:23PM ([#9177875](#))
that the US spies on its "friends" in the first place.

It may be naive, but if you want respect you have to give respect.

- **Re:What I find disturbing is...**

(Score:5, Interesting)

by [GauteL \(29207\)](#) on Monday May 17, @06:30PM ([#9177939](#))
(<http://lindkvis.blogspot.com/>)

True, it can't possibly be disturbing that the EU does not want the US spying on them after the US misused the trust completely during incidents like the Airbus/Boeing scandal.

You can't possibly question the motives of a country trying to protect against spies from friendly countries, when those friendly countries actually ARE spying on them.

[[Parent](#)]

- [Re:What I find disturbing is...](#) by NanoGator (Score:2) Monday May 17, @06:43PM
 - **Re:What I find disturbing is...**

(Score:5, Interesting)

by [Midnight Thunder \(17205\)](#) on Monday May 17, @06:52PM ([#9178172](#))
(<http://slashdot.org/> | Last Journal: [Saturday February 05, @04:50AM](#))
And the UK isn't spying on us?

From what I understand they are, but its scarier than you think. The US is not, in many instances, allowed to spy on its own citizens, so it makes use of any ally to do it for them. This means they get round any privacy issues. In return the US spies on the UK to give the UK information on their own citizens.

This based on what I have been told. If anyone has anything to prove or disprove this, please share here.

[[Parent](#)]

■ **1 reply** beneath your current threshold.

- [Re:What I find disturbing is...](#) by da5idnetlimit.com (Score:2) Monday May 17, @06:53PM
 - [Re:What I find disturbing is...](#) by Spunk (Score:1) Monday May 17, @07:01PM
- [Re:What I find disturbing is...](#) by DAldredge (Score:2) Monday May 17, @07:04PM

■ **1 reply** beneath your current threshold.

- [Re:What I find disturbing is...](#) by einnor (Score:2) Monday May 17, @06:31PM
- [Re:What I find disturbing is...](#) by kippy (Score:1) Monday May 17, @06:36PM
 - [Re:What I find disturbing is...](#) by drinkypoo (Score:2) Monday May 17, @06:48PM
 - [Re:What I find disturbing is...](#) by hugosantos (Score:1) Monday May 17, @06:51PM
 - [loss of privacy != more security](#) by aurelian (Score:1) Monday May 17, @06:56PM
- **Re:What I find disturbing is...**

(Score:5, Insightful)

by [Zak3056 \(69287\)](#) on Monday May 17, @06:39PM ([#9178037](#))
(<http://zak3056.livejournal.com/> | Last Journal: [Tuesday November 02, @09:06AM](#))
that the US spies on its "friends" in the first place.
It may be naive, but if you want respect you have to give respect.

There's no "may" to it, it's incredibly naive. Yep, the US spies on it's allies--but if you believe that those allies are not spying on the US in turn, you're dreaming. Charles de Gaulle once said that nations do not have friends--only interests. That's as true today as it was then.

[[Parent](#)]

- **Re:What I find disturbing is...**

(Score:5, Informative)

by [spun \(1352\)](#) <loverevolutionary@yahoo.com> on Monday May 17, @06:40PM ([#9178049](#))
(Last Journal: [Thursday May 18, @06:08PM](#))

Australia admitted the existence of Echelon, and it's part in the global surveillance network some years ago. The reason? The US demanded access to all data from Australia, whereas Australia wanted to remove the names of Australian citizens and businesses not under investigation. They would provide the details when asked, just not up front, to protect against the US using the info for corporate espionage. The Australians refused, the US said "Oh yeah, what are you gonna do?" and the Aussies responded, "Tell the world."

Here's [a link](#), [heise.de] but you can google 'echelon australia' for more info

[[Parent](#)]

- [Re:What I find disturbing is...](#) by Anonymous Coward (Score:1) Monday May 17, @06:42PM
- [Well Duh](#) by blunte (Score:2) Monday May 17, @06:50PM
 - [Re:Well Duh](#) by rokzy (Score:3) Monday May 17, @06:54PM
 - [Re:Well Duh](#) by blunte (Score:2) Monday May 17, @07:04PM
 - [Re:Well Duh](#) by rokzy (Score:3) Monday May 17, @07:11PM
- [Re:What I find disturbing is...](#) by EvanED (Score:2) Monday May 17, @06:58PM
- **Re:What I find disturbing is...**

(Score:5, Interesting)

by [j. andrew rogers \(774820\)](#) on Monday May 17, @07:09PM ([#9178340](#))

The majority of espionage conducted against the US is by our friends, largely from Europe. UK, France, and Germany being the major active players from Europe as I seem to remember. While it doesn't get wide press, the US catches (and then deports) several hundred European spies every year. How spies are treated depends

on what country they are from.

I remember over a decade ago when I actually worked in a business in which we were espionage aware, that the number one espionage problem in the US was the French (followed by the Chinese, and then a laundry list of European countries -- including the UK), the French being primarily interested in stealing US weapons technology and listening in on business deals they were competing with. Which was primarily a business move; along with the Russians and the US, the French are one of the world's major arms exporting countries and they have to compete with US designed weapons on the open market.

Everyone spies on everyone, and for varying reasons. The French actually used to have one of the most aggressive intelligence services on the globe, disproportionate to their size and geopolitical importance, which some people find surprising. I don't know if it as large today, though. But this is nothing new, and all the governments understand that this goes on. As long as it doesn't get out of hand, it is tolerated between countries that are nominally friendly.

[[Parent](#)]

- [Re:What I find disturbing is...](#) by Anonymous Coward (Score:1) Tuesday May 18, @06:44AM
 - **1 reply beneath your current threshold.**
- [Re:What I find disturbing is...](#) by amightywind (Score:2) Tuesday May 18, @08:23AM
 - [Re:What I find disturbing is...](#) by Abundantes (Score:1) Tuesday May 18, @10:45AM
- [Re:What I find disturbing is...](#) by The Lynxpro (Score:2) Tuesday May 18, @01:47PM
 - **1 reply beneath your current threshold.**
- [Re:What I find disturbing is...](#) by AxelTorvalds (Score:2) Monday May 17, @07:11PM
 - [Re:What I find disturbing is...](#) by Dravik (Score:1) Tuesday May 18, @12:02AM
- [Re:What I find disturbing is...](#) by esampson (Score:2) Monday May 17, @08:11PM
 - [Re:What I find disturbing is...](#) by Spectra72 (Score:1) Monday May 17, @10:32PM
 - [Re:What I find disturbing is...](#) by esampson (Score:1) Tuesday May 18, @03:11PM
 - [Re:What I find disturbing is...](#) by The Lynxpro (Score:2) Tuesday May 18, @02:00PM
 - [Re:What I find disturbing is...](#) by esampson (Score:1) Tuesday May 18, @03:14PM
 - [Re:What I find disturbing is...](#) by The Lynxpro (Score:2) Tuesday May 18, @04:47PM
- [Re:What I find disturbing is...](#) by G-funk (Score:2) Monday May 17, @09:41PM
- [Re:What I find disturbing is...](#) by Dravik (Score:1) Monday May 17, @11:50PM
- [Re:What I find disturbing is...](#) by d474 (Score:1) Tuesday May 18, @01:56AM
- [Re:What I find disturbing is...](#) by escallywag (Score:1) Tuesday May 18, @08:17AM
- **4 replies beneath your current threshold.**
- [Big Brothers](#) by Cheo (Score:2) Monday May 17, @06:24PM
 - [Re:Big Brothers](#) by gg3po (Score:1) Monday May 17, @06:30PM
 - [Re:Big Brothers](#) by angst_ridden_hipster (Score:2) Monday May 17, @06:59PM
 - [Re:Big Brothers](#) by Mathonwy (Score:2) Monday May 17, @08:03PM
- **"The political implications are troubling"?**

(Score:5, Insightful)

by [Saint Aardvark \(159009\) *](#) on Monday May 17, @06:25PM ([#9177887](#))
(<http://www.saintaardvarkthecarpeted.com/blog> | Last Journal: [Friday June 30, @08:05PM](#))

I beg your pardon? Why the *fuck* are the implications of taking up cryptography to stop shady, shouldn't-be-happening-in-the-first-place eavesdropping by so-called friends and allies "troubling"?

If there is a "growing rift" in the Western hemisphere, who the *fuck* do you think is responsible for this -- the ones who are pissed off about the eavesdropping and are trying to do something to stop it (and think for a moment about the fact that they're trying encryption rather than attempting to convince the US et al. that it's a Bad Thing...what does that tell you about their chances of actually convincing anyone to stop anything?), or *the countries and intelligence agencies that decided this was acceptable in the first place?*

Sorry for the shouting, but this intellectual coyness does *not* become you.

- [Re:"The political implications are troubling"?](#) by Dark Lord Seth (Score:2) Monday May 17, @06:37PM
 - [Re:"The political implications are troubling"?](#) by Daniel Dvorkin (Score:2) Monday May 17,

@06:47PM

- [Re:"The political implications are troubling"?](#) by Kirill Lokshin (Score:3) Monday May 17, @06:45PM
- [Re:"The political implications are troubling"?](#) by Tripster (Score:2) Monday May 17, @06:50PM
 - [Re:"The political implications are troubling"?](#) by mebon (Score:1) Monday May 17, @07:26PM
 - [Re:"The political implications are troubling"?](#) by DeLanceS (Score:2) Tuesday May 18, @01:12AM
- [Re:"The political implications are troubling"?](#) by J'raxis (Score:2) Monday May 17, @10:16PM
- [Re:Eloquent? Fuck no...](#) by Saint Aardvark (Score:2) Monday May 17, @07:09PM
- [2 replies beneath your current threshold.](#)
- **That sounds kind of silly**

(Score:5, Insightful)

by [Noose For A Neck \(610324\)](#) on Monday May 17, @06:25PM (#9177888)

While I'm sure it sounds well and good to a legislator in the EU when they hear about supposedly "unbreakable" quantum cryptography, this sounds like another case of someone mistaking it for some kind of panacea for eavesdropping. The real truth of the matter is that, of course, quantum crypto is only effective at the *line level*, i.e. as soon as it leaves the medium it was transmitted on, the cryptographic effect is lost. So it's entirely impractical for anything but a point to point connection.

Also, I don't think people realize how strong cryptography is today. There are cryptographic methods available to the public at large (such as RC5 and PGP) that are proven to require more computing power than is theoretically possible in the universe. Not just more computing power than is possible with current hardware, but the *theoretical limits of computation given the entire resources of the universe*. So really, it seems that a lot of ignorance is at play here, and I would hope someone clueful in the EU informs their EU government before they go off and waste a whole lot of taxpayer money on such a foolish project.

- **Re:That sounds kind of silly**

(Score:4, Insightful)

by [skifreak87 \(532830\)](#) on Monday May 17, @06:38PM (#9178032)

Sorry to nitpick, but it takes "more computing power than is theoretically possible in the universe" assuming no better algorithm for breaking the encryption is developed. If someone creates a polynomial time algorithm for factoring large numbers (such as Shor's algorithm for quantum computers), this is no longer the case for RSA or any other factoring vs. multiplying/generating primes system. Similarly for other systems. It's not that the system cannot be broken, it's that we don't know of a way in which it can be done using current algorithms. The only informationally secure encryption system (afaik) is a never re-used one-time pad because it makes all decryptions equally likely and thus you gain NO information about the cleartext from the encrypted text except possibly length. The problem is, this requires a truly random key at least as long as the length of the message and the key cannot be reused.

[[Parent](#)]

- **Re:That sounds kind of silly**

(Score:5, Interesting)

by [calv1n \(135902\)](#) <snookNO@SPAMguanotronic.com> on Monday May 17, @06:41PM (#9178058)

This is only true using a full-keyspace brute force attack. The NSA was at least 20 years ahead of the academic world in discovering linear cryptanalysis. This is why they asked IBM to change the sboxes in DES, but wouldn't say why. The result was that DES was using an sbox from a fairly small subset of possible sboxes that resist linear cryptanalysis, but we didn't know it for another couple decades. Imagine for a minute that the NSA had a technique that cut the effective key size by a factor of 4. You can brute force attack that. There might even be polynomial algorithms for it, taking advantage of mathematical properties that only the largest employer of mathematicians in the world knows about.

We can't even be certain that the NSA doesn't have quantum computers, although this is less likely. When your attacker has a non-deterministic computer, you're fairly screwed on finding an algorithm that can be efficiently encoded and decoded on deterministic machines while taking extraordinarily long to decrypt without the key. The only saving grace here is that a quantum computer may not be a general non-deterministic machine, so there may be some things that a non-deterministic machine can do that a quantum computer cannot. To my knowledge, the equivalence between quantum computers and non-deterministic

machines has not been proven either positively or negatively. I'm sure the NSA knows though.

[[Parent](#)]

- **1 reply beneath your current threshold.**

- [Re:That sounds kind of silly](#) by bfields (Score:3) Monday May 17, @06:44PM
- [Re:That sounds kind of silly](#) by Karhgath (Score:3) Monday May 17, @06:49PM
 - [I've been wondering...](#) by arafel (Score:1) Tuesday May 18, @09:33AM
- [Re:That sounds kind of silly](#) by moreati (Score:3) Monday May 17, @06:50PM
- [Re:That sounds kind of silly](#) by jd (Score:2) Monday May 17, @07:04PM
- [Re:That sounds kind of silly](#) by esampson (Score:2) Monday May 17, @08:40PM
 - [Re:Oh shut up.](#) by esampson (Score:1) Tuesday May 18, @03:32PM
 - **1 reply beneath your current threshold.**
- [Re:That sounds kind of silly](#) by slimslam (Score:1) Tuesday May 18, @02:54AM
- [Re:That sounds kind of silly](#) by escallywag (Score:1) Tuesday May 18, @10:41AM
- **1 reply beneath your current threshold.**
- [Easy Solution](#) by dunelin (Score:2) Monday May 17, @06:25PM
 - [Re:Easy Solution](#) by stanmann (Score:1) Tuesday May 18, @07:49AM
- [Sounds stupid...](#) by Hobbex (Score:2) Monday May 17, @06:27PM
 - [Re:Sounds stupid...](#) by JamesKPolk (Score:3) Monday May 17, @06:30PM
 - [Re:Sounds stupid...](#) by Sanity (Score:2) Monday May 17, @06:31PM
 - **Re:Sounds stupid...**

(Score:5, Insightful)

by [Hobbex \(41473\)](#) on Monday May 17, @06:51PM ([#9178157](#))

Perhaps, but then again, how many respected Nazi researchers believed that the allies had cracked the Enigma code?

It was not unreasonable for them to have suspected so. The integrity of Enigma relied heavily on keeping the machines and codebooks out of allied hands - had the Germans known that the allies had managed to get ahold of those things, the impressive effort of Turing & co. to go the last bit would not have been inconceivable to his German counterparts.

If the NSA can really crack any of our modern cryptographical methods, then they are at least forty fifty years ahead of the rest of world in both mathematics and computing. Is that conceivable? And if they are, then they can't really do anything with what they find anyways, since they would have to spend most of their energy keeping the secret.

Basically you are trying to score cheap points (read karma) but making a comparison that doesn't hold, but that plays on peoples emotions. It's the equivalent of responding to any comment advocating avoiding war with: "That's what Chamberlain thought."

[[Parent](#)]

- [Re:Sounds stupid...](#) by Sanity (Score:2) Monday May 17, @06:56PM
- [Re:Sounds stupid...](#) by esampson (Score:1) Monday May 17, @08:43PM
- [Re:Sounds stupid...](#) by pipingguy (Score:2) Monday May 17, @11:01PM
- [Re:Sounds stupid...](#) by stanmann (Score:1) Tuesday May 18, @07:52AM
- **1 reply beneath your current threshold.**
- **1 reply beneath your current threshold.**
- [Re:Sounds stupid...](#) by MrIrwin (Score:2) Monday May 17, @06:50PM
 - [Re:Sounds stupid...](#) by Trelane (Score:2) Monday May 17, @08:18PM
 - [Re:Sounds stupid...](#) by MrIrwin (Score:2) Tuesday May 18, @02:37AM
- **3 replies beneath your current threshold.**
- **The UK's role in the EU**

(Score:5, Insightful)

by [nickos \(91443\)](#) on Monday May 17, @06:27PM ([#9177911](#))

As someone who lives in the UK, I think our stance on this is ridiculous, and a legacy of WW2. We're an important and influential member of the EU, and the last couple of years should have made it obvious that a close relationship with the US damages our relationship with the rest of Europe (and the wider world) and only benefits the Americans.

In the post Empire world, Britain's role is as a democratic and decent European nation. We should not support preemptive war or the Israeli's mistreatment of the native Palestinians.

Oi, Blair! Sort it out.

- [Re:The UK's role in the EU](#) by twigles (Score:1) Monday May 17, @07:00PM
 - [Re:The UK's role in the EU](#) by Erik_ (Score:2) Monday May 17, @07:04PM
 - **1 reply beneath your current threshold.**
- [Re:The UK's role in the EU](#) by The Lynxpro (Score:2) Tuesday May 18, @02:14PM
 - [Re:The UK's role in the EU](#) by nickos (Score:2) Tuesday May 18, @07:03PM
 - [Re:The UK's role in the EU](#) by The Lynxpro (Score:2) Tuesday May 18, @07:30PM
- **Re:The UK's role in the EU**

(Score:4, Informative)

by [nickos \(91443\)](#) on Monday May 17, @06:42PM ([#9178069](#))

Look, the fact is that even in the EU countries whose governments support the US, the majority of the electorate are against the US's mis-adventures in the middle east. Even in America the people are turning against the Iraqi war. No-one is lying - some governments in Europe are openly against the war, while others have obviously supported it.

The interesting thing is that the majority of people in all of these countries are against the Iraqi war.

[[Parent](#)]

- [Re:The UK's role in the EU](#) by Alci12 (Score:1) Monday May 17, @08:19PM
- **Re:The UK's role in the EU**

(Score:5, Insightful)

by [rduke15 \(721841\)](#) <[rduke15\(at\)gmail.com](mailto:rduke15(at)gmail.com)> on Monday May 17, @09:12PM ([#9179266](#))

A simpler statement might be that a good majority of the EU population are anti-American irrespective of what they do

That is not true. Anybody who knows Europe will be able to tell you that the Iraq war made a **huge** difference.

While before, a tiny minority was anti-American, it seems to have grown to the vast majority only because of the Iraq war. Anti-Americanism has now become so pervasive in the European society, that I even hear it in remarks from my kids. And they are at an age (8) when their views are ultra-conservative, and they would only express things that are shared by a significant majority in the school yard.

Believe me, Americans are only fooling themselves if they ignore the damage this war (or this administration) has done to their country.

[[Parent](#)]

- [Re:The UK's role in the EU](#) by Alci12 (Score:1) Monday May 17, @09:44PM
- **Re:The UK's role in the EU**

(Score:4, Insightful)

by [dunkelfalke \(91624\)](#) on Tuesday May 18, @05:00AM ([#9181198](#))

<http://www.speznas.de/>

chechnya is still a part of russian federation.

but i somehow missed that iraq was an us state.

[[Parent](#)]

- [Re:The UK's role in the EU](#) by Alci12 (Score:1) Tuesday May 18, @08:18AM
- [Re:The UK's role in the EU](#) by radja (Score:2) Tuesday May 18, @05:16AM
 - [Re:The UK's role in the EU](#) by Alci12 (Score:1) Tuesday May 18, @08:25AM
 - **1 reply beneath your current threshold.**
- **Anti-american kids**

(Score:4, Insightful)

by [zoney_ie \(740061\)](#) on Tuesday May 18, @04:43AM (#9181152)

Yep. I too am somewhat alarmed at the immediate opinions expressed of "America" by kids here (Ireland). It's all well and good us University students debating current affairs and bashing US foreign (and domestic) policy, but when enough ill-feeling has spread that those who do not understand or follow all the issues are influenced - it's time to get worried.

As long as things continue as they are going, I'm sorry folks, but the US is going to be less and less respected in Europe. Unfortunately, people will also begin (continue?) to blur the line between the government and people.

In fact, I would be more Anti-American than I am now, were it not for making some American friends last year (during the Iraq invasion of all times!) and going over to the US for the first time to visit.

People will easily forget all the great and wonderful things about the US. Hatred and ill-feeling is much more persuasive.

The US government's direction needs to change. Probably more than just switching to Kerry! (A more democratic voting system would be a good start!)

[[Parent](#)]

- [Re:The UK's role in the EU](#) by joonasl (Score:3) Tuesday May 18, @03:50AM
 - [Re:The UK's role in the EU](#) by stanmann (Score:1) Tuesday May 18, @07:56AM
 - [Re:The UK's role in the EU](#) by jsebrech (Score:2) Tuesday May 18, @08:00AM
 - [Re:The UK's role in the EU](#) by stanmann (Score:1) Tuesday May 18, @09:30AM
 - [Re:The UK's role in the EU](#) by The Lynxpro (Score:2) Tuesday May 18, @02:23PM
 - [Re:The UK's role in the EU](#) by joonasl (Score:2) Wednesday May 19, @01:47AM
- **Re:The UK's role in the EU**

(Score:5, Insightful)

by [jsebrech \(525647\)](#) on Tuesday May 18, @08:57AM (#9182203)

Nice to know that having good relations with the likes of Saddam is viewed more important than having good relations with USA.

I understand people might disagree about ways to remove/contain a dangerous dictator but to completely turn this issue into US hate-fest is something completely different.

Ok, second point first. The anti-americanism in my view (as a belgian citizen) could more appropriately be called anti-bushism. My 16yo sister wants to go to the US, because she thinks it's a great country, but George W. Bush is number one on her hate list. So, no, from my perspective there is no US hate-fest. This might be different in other countries though. I can imagine the french not being happy with how they have been treated over the past few years.

As to wanting better relations with Saddam than with the US. Do you honestly believe that? It is just plain silly. The problem Europe had was not that they thought we should all be friends with Saddam, it was that war should be a last resort. The reason given prior to the Iraq invasion, weapons of mass destruction, was generally known over here to be a bogus reason. Even if there were wmd's (which we now know there weren't) then it would have been better to let the UN inspectors find them. Instead, the US went on a pointless and unfounded smear campaign against the inspectors (on-going to this day), and then said that war was the only way to get things done in iraq, which was a lie. As an aside, do you believe Saddam was an immediate threat to the US, and if so, why?

After the war, the reason given became iraqi freedom, but at the same time we're seeing the iraqi's do not have control over their own natural resources (oil production and profits are

entirely in US hands), do not have control over their own financial resources (all the government money is in US hands), and do not have control over the political decisions taken (a power which is supposed to be handed over soon, but nobody knows to whom, and the resources to use that power aren't coming along with it). Not to mention that if you hold Iraq as the standard for countries in need of liberation, you need to go liberate half the world, including current US allies, like China (which is a dictatorship with a horrible human rights record, and a history of invading other countries, just like Iraq).

The US is the most powerful democracy in the world, and as a result, the EU holds it to a very high standard. We expect moral leadership from the US, and the whole Iraq situation is such a disgrace to the US that we have problems understanding why the American public would back an administration that makes such poor decisions. The loud criticism of the US you've heard is our way of saying "we expect better of you, now go do something about it!"

Europe is not US ally anymore.

Europe definitely wants to be a US ally, but the Bush administration has made it really really hard, with all kinds of anti-european economic policies (which is being called a "trade war" in the international press), a unilateral withdrawal from many treaties which Europe considers crucial (Kyoto, the international criminal court, the treaties on chemical and biological weapons, the nuclear disarmament treaties, and so on...), and a general smear campaign against any EU country which dares voice political opposition ("that's old Europe", remember that one?).

You have to treat people with respect to get respect back. All the US needs to do to have a strong ally in Europe is to do what it claims to stand for.

I still remember Aznar speech in which he described the secret rejoicing of various Europeans politicians he witnessed in the months after 9/11 - especially of the "that's what you get for supporting Israel" type.

I never heard that. If he did say it, and if it is true, then I wouldn't be surprised by it. 9/11 IS a direct consequence of US middle east policy over the last few decades. Osama himself has said the primary reason for him was the US mili

[Read the rest of this comment...](#)

[[Parent](#)]

- [Re:The UK's role in the EU](#) by jsebrech (Score:2) Tuesday May 18, @12:22PM

- **1 reply** beneath your current threshold.

- **3 replies** beneath your current threshold.

- **1 reply** beneath your current threshold.

- [Re:The UK's role in the EU](#) by Daniel Dvorkin (Score:2) Monday May 17, @06:55PM

- **3 replies** beneath your current threshold.

- [Terrorists](#) by Lefte (Score:3) Monday May 17, @06:29PM

- [Re:Photon Cables](#) by Lefte (Score:1) Monday May 17, @06:47PM

- **1 reply** beneath your current threshold.

- **1 reply** beneath your current threshold.

- [Ronald Reagan did a few good things](#) by SeanTobin (Score:2) Monday May 17, @06:32PM

- [Re:Ronald Reagan did a few good things](#) by Rosco P. Coltrane (Score:3) Monday May 17, @06:36PM

- [Re:Ronald Reagan did a few good things](#) by HBI (Score:1) Monday May 17, @06:46PM

- [It's all about money...](#) by Erik_ (Score:2) Monday May 17, @07:10PM

- [Re:Ronald Reagan did a few good things](#) by rocketfairy (Score:2) Monday May 17, @08:02PM

- [Re:Ronald Reagan did a few good things](#) by Anonymous Coward (Score:1) Monday May 17, @08:29PM

- [Re:Ronald Reagan did a few good things](#) by cs (Score:1) Sunday May 23, @11:16PM

- [Re:Ronald Reagan did a few good things](#) by Anonymous Coward (Score:1) Monday May 17, @07:04PM

- [Re:Ronald Reagan did a few good things](#) by Trelane (Score:2) Monday May 17, @08:33PM

- **1 reply** beneath your current threshold.

- **How it came to pass...**

(Score:5, Funny)

by Anonymous Coward on Monday May 17, @06:34PM ([#9177979](#))

```
*** Schroder ( ~schroder!blinky@reichstag.de ) has joined #europe
*** TOPIC: Be nice to the new guys or Ireland will export drunk hooligans to your
country!
<Schroder> Gutentag!
<Blair> Cheerios, ol' chap!
<Chirac> Sup?
<Schroder> What's happening over here?
<Chirac> Just watching zat goddamn idiot Bush trying to lose a war.
<Schroder> Ach so...
*** Bush ( ~bush!dubya@whitehouse.gov ) has joined #europe
<Bush> I READ THAT, YOU BITCH!!!
*** Bush has left #europe
<Schroder> Right, this is getting tiresome...
<Blair> Fancy a crumpet, anyone?
```

- **[1 reply](#) beneath your current threshold.**
- [Statecraft 101](#) by Anonymous Coward (Score:2) Monday May 17, @06:35PM
 - [Switzerland, 4 langues, 703 years of existance](#) by Erik_ (Score:2) Monday May 17, @07:18PM
 - [Re:Statecraft 101](#) by trewoman (Score:2) Monday May 17, @07:50PM
 - [Re:Statecraft 101](#) by stanmann (Score:1) Tuesday May 18, @08:10AM
 - [Re:Statecraft 101](#) by Rumagent (Score:2) Tuesday May 18, @01:29AM
 - **[1 reply](#) beneath your current threshold.**
- [Pure snake oil](#) by Paul Johnson (Score:3) Monday May 17, @06:35PM
 - [Re:Pure snake oil](#) by Trelane (Score:2) Monday May 17, @07:25PM
 - [Re:Pure snake oil](#) by Paul Johnson (Score:2) Monday May 17, @11:29PM
 - [Re:Pure snake oil](#) by Sweetshark (Score:1) Tuesday May 18, @09:00AM
 - [Re:Pure snake oil](#) by Sweetshark (Score:1) Monday May 17, @07:34PM
 - [Re:Pure snake oil](#) by Paul Johnson (Score:2) Monday May 17, @11:25PM
 - [Re:Pure snake oil](#) by Sweetshark (Score:1) Tuesday May 18, @07:38AM
 - [Re:Pure snake oil](#) by Paul Johnson (Score:2) Monday May 17, @11:32PM
 - **[1 reply](#) beneath your current threshold.**
- **Buzzwords**

(Score:5, Insightful)

by [flossie \(135232\)](#) on Monday May 17, @06:36PM ([#9178004](#))

(<http://www.writetothem.com/>)

I'm pleased that there is funding for this kind of research in the EU, but it sounds like a stupid way of solving the problem of Echelon. The article makes it clear that the purpose of the quantum encryption is to exchange keys securely and to then encrypt messages using more conventional algorithms and transmission methods.

If conventional encryption and transmission is deemed sufficiently secure for transmitting the messages, a quantum exchange of keys does not add significantly to the security of the communication. It would surely be easier and cheaper to organize physical transfer of one-time pads than to install all the necessary infrastructure to support the key exchange.

The EP were obviously taken in by buzzwords, but at least the research will advance the state of the art.

- [Re:Buzzwords](#) by Karhath (Score:2) Monday May 17, @07:09PM
- [All Your Base Are Belong To Us...](#) by greyfeld (Score:2) Monday May 17, @06:36PM
 - [Re:All Your Base Are Belong To Us...](#) by Anonymous Coward (Score:1) Monday May 17, @06:55PM
 - [You mean: All Your Data Belong To U.S.](#) by CognitiveFusion (Score:1) Monday May 17, @10:42PM
- [EU spin on economic espionage](#) by LinuxParanoid (Score:1) Monday May 17, @06:37PM
 - [Spin](#) by exp(pi*sqrt(163)) (Score:2) Monday May 17, @06:55PM
- [Oh, please.](#) by e9th (Score:1) Monday May 17, @06:37PM

- o [Re:Oh, please.](#) by Dan Farina (Score:1) Monday May 17, @10:11PM
- [You Have Quantum Mail!](#) by 10101001011 (Score:3) Monday May 17, @06:39PM
 - o [Re:You Have Quantum Mail!](#) by 10101001011 (Score:1) Monday May 17, @07:14PM
 - o **1 reply beneath your current threshold.**
- **Useless until they have quantum routers**

(Score:4, Insightful)

by [G4from128k \(686170\)](#) on Monday May 17, @06:39PM ([#9178045](#))

Although quantum crypto secures the fiber, it does nothing for the equipment on either end. Routers, switches, ISP mail servers, etc. remain accessible.

Until Linksys sells a consumer quantum WAN interface, CISCO sells quantum Layer 3 switches, and all the telcos fiber-up with quantum crypto repeaters, the whole system is vulnerable to snooping.

- o [Re:Useless until they have quantum routers](#) by Karhgath (Score:2) Monday May 17, @07:40PM
 - [Quantum routers and encryption franchises](#) by G4from128k (Score:3) Monday May 17, @08:01PM
 - [Re:Quantum routers and encryption franchises](#) by Karhgath (Score:2) Monday May 17, @08:13PM
 - [Re:Quantum routers and encryption franchises](#) by P-Nuts (Score:1) Tuesday May 18, @09:11AM
 - [Re:Useless until they have quantum routers](#) by pherris (Score:2) Monday May 17, @09:01PM
 - [Quantum Teleportation](#) by jpmorgan (Score:2) Tuesday May 18, @03:55PM
- **Secure Systems**

(Score:5, Informative)

by [BrownDwarf \(615206\)](#) on Monday May 17, @06:44PM ([#9178094](#))

The weakness in current encryption/communications systems isn't in the encrypting algorithms, which have withstood the serious efforts of some top-flight mathematicians to bust them. Nor is it necessarily in traffic analysis; keep a line open and transmitting bits 24/7. Isn't hard to design the system so the intended recipient can tell when the "random" bits start a message. Nor is the weakness in key transmission, at least for governments: lots and lots of really long keys can be transported on CDs well in advance of need. The weakness remains where it has been in recent years, with the people using the system, and with keeping their computers out of unauthorized hands. Going to quantum methods doesn't change get around this weakness. From what I see, the benefit of quantum crypto is the ability to make message tampering evident.

- [A question...](#) by dfj225 (Score:2) Monday May 17, @06:45PM
 - o [Re:A question...](#) by Kirill Lokshin (Score:2) Monday May 17, @07:03PM
 - o **1 reply beneath your current threshold.**
- [Is the NSA behind it?](#) by Florian Weimer (Score:2) Monday May 17, @06:56PM
 - o **Re:Is the NSA behind it?**

(Score:5, Informative)

by [Karhgath \(312043\)](#) on Monday May 17, @07:28PM ([#9178513](#))

Well, I won't say you're a troll, but probably missinformed.

Quantum cryptography has a cool name, but in practice, it sucks, at least its current implementations.

Ok, that's right. But it sucks not because it's flawed, but because it's too slow to communicate with yet(well, to create the key actually).

It's not end-to-end by design (you can't have a direct fiber to everyone you want to communicate with these days, after all), and so it's easily regulated.

More current implementations use 'wireless' quantum channels in open air, so it isn't restricted to fiber only. I agree that you won't have consumer implementation before at least 8-10 years, but if a big corporation or government wants to use it, they will be able to in the near future.

It's expensive.

Sure. Is there a new technology that isn't expensive? Is that incentive enough to stop developing new ideas and such? No.

It doesn't solve key management problems, and the installations that have been publicly described so far are extremely vulnerable to man-in-the-middle attacks.

WOAH! Until then it was ok, just some argumentation problems, but this is pure outright misinformation. I don't know where you read that, I'd like to know.

First, Quantum Key Distribution is there to SOLVE key management problems related to one-time pad methods. The first and foremost goal of quantum encryption is to remove the logistic problems of one-time pad. So, you are wayyy off on this one.

Second, QKD is unconditionally secure, and that includes man-in-the-middle. I doubt current implementation are "extremely vulnerable" against that attack, unless you have some proof to show, I'd be interested to know.

If I believed in conspiracy theories, I'd say that the NSA is luring the EU towards unavailable and untested quantum cryptography, and away from commercially available, tested, reliable and rather secure conventional crypto products. Actually, the quantum crypto recommendation (whether it's contained in some EU documents or not) is the result of a pretty slick PR (and lobbying) campaign.

Well, I can't argue about tin-foiled hat arguments, hehe. The problem with conventional crypto methods is that they are breakable in the absolute, and the Echelon program is certainly the one who is able to achieve this feat. QKD isn't. This is the main point in favor of QKD, especially when you want to protect yourself against Echelon.

[[Parent](#)]

- [Re:Is the NSA behind it?](#) by Trelane (Score:3) Monday May 17, @08:52PM
 - [Re:Is the NSA behind it?](#) by The Cookie Monster (Score:2) Tuesday May 18, @09:22AM
 - [Re:Is the NSA behind it?](#) by Florian Weimer (Score:2) Wednesday May 19, @03:26AM
 - **1 reply beneath your current threshold.**
 - [Re:Is the NSA behind it?](#) by Florian Weimer (Score:2) Wednesday May 19, @03:14AM
- [Other eavesdropping systems...](#) by cepheusfilms (Score:1) Monday May 17, @06:59PM
 - [Re:Other eavesdropping systems...](#) by Orne (Score:2) Monday May 17, @10:00PM
- [Mass encryption](#) by t_allardyce (Score:3) Monday May 17, @07:06PM
- [In other news ..](#) by DrugCheese (Score:3) Monday May 17, @07:06PM
 - [Willful blindness. . .](#) by Fantastic Lad (Score:2) Tuesday May 18, @04:53AM
- [If this is true about Echelon...](#) by Castaa (Score:1) Monday May 17, @07:10PM
 - **1 reply beneath your current threshold.**
- **Missing the point**

(Score:5, Insightful)

by [maximilln \(654768\)](#) on Monday May 17, @07:11PM ([#9178366](#))

(<http://www.linuxfromscratch.org/> | Last Journal: [Friday August 27, @07:36AM](#))

Everyone--from good hearted people to downright argumentative trolls--misses the point on spying.

I don't care about online privacy. I'm not worried about government spooks sifting through my e-mail or web surfing habits and finding out that I like brunettes with long legs, long hair, and almond shaped eyes. It really doesn't concern me. If it were some supercomputer sitting in a back room chewing through e-mail looking for "homicide, suicide, terror, assassinate, secret, password, 9/11" or some other stupid set of keywords or tracing kiddie porn that'd be fine by me. At least until the anti-pr0n people decide that moral righteousness has no bounds and start coming after willing adults with no real sex life and a speedy net connection.

Face it. We live in the real world. People in power let it go to their heads and they often use it for purposes other than those in which it was given to them for.

What I'm worried about is that the guy down the block is an FBI agent. Or CIA. Or NSA. Or some local politician who knows one. One day I'm walking down the street and a candy wrapper drops out of my pocket onto his lawn. Now this guy is such a straight laced Bible thumping tight a__ POS that he uses his political muscle to find out who I am and begin harassing me. "He dropped a candy wrapper on my lawn! He's a litterer! He's no good for society! Besides, I saw him carrying home a six-pack of beer! He must be an alcoholic as well!"

Where's the check and balance? There is none. Who could prove it? No one. Who can stop it? No one.

Echelon, Big Brother surveillance, the Anti-Terror bill. They all suck for the same reason that the Windows registry sucks: there's no way to secure them from people misusing them to hijack the system.

- [Re:Missing the point](#) by Anonymous Coward (Score:1) Monday May 17, @07:27PM
 - [Re:Missing the point](#) by maximilln (Score:3) Monday May 17, @08:08PM
 - **1 reply beneath your current threshold.**
- **1 reply beneath your current threshold.**
- [the naivete of people astounds me.](#) by jerky42 (Score:2) Monday May 17, @07:23PM
- **Two Books to understanding Echelon**

(Score:5, Informative)

by [braddock \(78796\)](#) on Monday May 17, @07:28PM ([#9178515](#))

There are two fantastic well-researched books that anyone who wishes to truly understand Echelon needs to read:

[Body of Secrets: Anatomy of the Ultra-Secret National Security Agency](#) [amazon.com] by James Bamford is a fantastic history of the NSA from the end of WWII to the present. If you read this book you will see that the idea that the NSA is spying on UN delegations is really a given...in fact one of the primary reasons the US wanted the UN to locate in NYC is to allow easy interception of diplomatic communications. This author uncovered many amazing Cold War programs and antidotes and presents them in fascinating form.

The second book is ["Blind Mans Bluff: The Untold Story of American Submarine Espionage"](#) [amazon.com] by Sherry Sontag, another fantastic book of solid research and good story telling, a large amount of it revolving around underwater communication wiretap activities. The special mission nuclear submarine SSN-21 USS Jimmy Carter is out there specially equipped for undersea cable tapping operations and receiving commendations in the tradition of the Cold War era [USS Halibut](#) [earthlink.net].

Whatever you think of the ethics of these issues, the technology and history is amazing, and the capabilities do exist and are fairly well documented. If you read these two books, and have the technological understanding to extrapolate a bit, you can get a pretty good picture of current capabilities and the culture of how these collection assets are being used. One thing you will find that they are not being used without limits and elements of responsibility, although there are cases (like the Boeing/Airbus bidding incident) where they have been abused.

-braddock gaskill

- [One more good book to add...](#) by weedenbc (Score:3) Monday May 17, @08:46PM
- [Re:Two Books to understanding Echelon](#) by BCW2 (Score:3) Monday May 17, @11:22PM
- [healthy competition](#) by Doc Ruby (Score:3) Monday May 17, @07:35PM
 - [Re:healthy competition](#) by JamesKPolk (Score:1) Monday May 17, @07:42PM
 - [Re:healthy competition](#) by Doc Ruby (Score:2) Monday May 17, @07:54PM
- [No Problem](#) by hardcode57 (Score:1) Monday May 17, @07:41PM
- [Great for stuff that goes along the Q.E. backbone](#) by Anonymous Coward (Score:1) Monday May 17, @08:03PM
- [Isn't the downside](#) by m1chael (Score:1) Monday May 17, @08:26PM
- [Banning of strong encryption](#) by nurb432 (Score:2) Monday May 17, @08:41PM
 - [Re:Banning of strong encryption](#) by KnightStalker (Score:3) Monday May 17, @09:21PM
 - [Re:Banning of strong encryption](#) by applemasker (Score:2) Tuesday May 18, @09:27AM
- [What EU?](#) by TheOtherKiwi (Score:1) Monday May 17, @09:15PM
- [No political implications](#) by BlightThePower (Score:3) Monday May 17, @11:25PM
- [Might spam protect us?](#) by hains (Score:1) Tuesday May 18, @02:07AM
 - [people are the weak link](#) by pensivemusic (Score:1) Tuesday May 18, @11:40AM
- [Is it possible?](#) by hcetSJ (Score:3) Tuesday May 18, @02:35AM
- [troubling?](#) by VanillaCoke420 (Score:2) Tuesday May 18, @04:25AM
- [UK and Echelon](#) by alex_tibbles (Score:1) Tuesday May 18, @05:16AM
- [EU, Crypto and Echelon](#) by LinuxLover (Score:1) Tuesday May 18, @07:27AM
 - [Re:EU, Crypto and Echelon](#) by pensivemusic (Score:1) Tuesday May 18, @11:06AM
- [Kind of lame](#) by Oestergaard (Score:3) Tuesday May 18, @08:18AM
- [what they are already doing in France...](#) by Frédéric (Score:2) Tuesday May 18, @09:10AM
- [Re:British double agents?](#) by Anonymous Coward (Score:2) Monday May 17, @06:43PM

- [I DID IT!!](#) by bsDaemon (Score:2) Monday May 17, @06:43PM
 - [1 reply](#) beneath your current threshold.
- [Re:What Americans & upper-class British fail t](#) by Trelane (Score:2) Monday May 17, @08:37PM
- [14 replies](#) beneath your current threshold.
-

Immature poets imitate, mature poets steal. -- T.S. Eliot, "Philip Massinger"

All trademarks and copyrights on this page are owned by their respective owners. Comments are owned by the Poster. The Rest © 1997-2007 [OSTG](#).